INFORME DE COMUNICA-BRECHA RGPD

Comunica-Brecha RGPD es una ayuda a la toma de decisiones sobre la obligación de comunicar una brecha de datos personales a los interesados afectados, pero estas últimas corresponden ineludiblemente al responsable de tratamiento y en ningún caso este informe representa el pronunciamiento de esta Agencia sobre la aplicación del art. 34 del RGPD para una brecha de datos personales concreta.

Puede obtener información más detallada aquí.

I. DATOS DEL RESPONSABLE Y DEL TRATAMIENTO

(A cumplimentar por el responsable para completar el informe)

Fecha: 05/02/2024

Usuario de la herramienta: LUIS MARÍA GOMEZ GUERRERO

Cargo: Representante para el COFRM del Delegado de Protección de Datos, PSN Sercon

Responsable del tratamiento

Identidad: COLEGIO OFICIAL DE FARMACÉUTICOS DE MURCIA

NIF: Q3066003I

Dirección postal: C\ JAIME I EL CONQUISTADOR Nº1 ENTRESUELO, 30008 MURCIA

Correo electrónico: protecciondedatos@cofrm.com

Teléfono: 968277400

Finalidad del tratamiento: Gestión de los servicios colegiales en materia fiscal y contable.

II. DATOS PROPORCIONADOS EN EL PROCESO DE EVALUACIÓN

La evaluación se ha obtenido con base en las siguientes respuestas facilitadas por el responsable en la herramienta:

1.- Indique el sector de actividad del responsable de tratamiento:

Otros sectores de actividad

2.- El incidente ha sido:

Accidental o sin intencionalidad

3.- El origen del incidente ha sido:

Interno: Personal o sistemas del responsable de tratamiento

4.- ¿La brecha de seguridad es consecuencia de un ciberincidente?:

No

5.- Como consecuencia del incidente:

- Personas u organizaciones que no están autorizadas, o no tienen un propósito legítimo para acceder a los datos, han podido acceder y/o extraerlos.

6.- Referido específicamente a los datos afectados. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?

No

9.- ¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas afectadas?:

Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

10.- A fecha de esta notificación, ¿tiene constancia de que se haya materializado alguno de los daños identificados, con el grado indicado en la cuestión anterior?

No

11.- Cómo valora la probabilidad de que el daño anterior se materialice sobre las personas afectadas con la severidad indicada?

Improbable

12.- Tipos de datos afectados. Seleccione los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables:

- Documento identificativo (Ej: DNI, NIE, pasaporte).
- Datos económicos o financieros (sin medios de pago).

13.- Entre las personas afectadas, ¿hay menores?:

No

14.- Entre las personas afectadas, ¿hay miembros de colectivos vulnerables como víctimas de violencia de género o en riesgo de exclusión social?:

No

15.- En total, ¿cuántas personas han visto sus datos afectados por la brecha de seguridad? (Si desconoce el valor exacto, indique un número aproximado/estimado):

592

16.- Indique la fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto afectados datos personales:

02/02/2024

17.- ¿Conoce la fecha en la que se inició la brecha?:

La fecha exacta

18.- Indique la fecha de inicio de la brecha:

01/02/2024

III. RESULTADO DE LA EVALUACIÓN

Evaluación realizada con fecha 05-02-2024 a las 11:01:18.

Según los datos facilitados,

NO SERÍA NECESARIO COMUNICAR LA BRECHA DE SEGURIDAD A LOS AFECTADOS

Conforme al atr. 34 del RGPD al no apreciarse que pueda existir un riesgo alto o muy alto para los derechos y libertades de los sujetos afectados. No obstante, podría valorar hacerlo de forma voluntaria, como ejercicio de transparencia y responsabilidad proactiva.