- **Expediente N.º: EXP202416691**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR RECONOCIMIENTO DE RESPONSABILIDAD Y PAGO VOLUNTARIO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 20 de diciembre de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA*** (en adelante, ***FSOM***), mediante el acuerdo que se transcribe:

<<
Expediente N.º: EXP202416691

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: La **FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA**, con NIF **G07324239** (en adelante, FSEOM) promovió la realización del ******PROYECTO.1***, con el objetivo de ***(…)***. Los datos eran recogidos por el propio paciente en una aplicación móvil en la que se registraba mediante un código que le suministraba su oncólogo médico. ***(…)***

Para la realización de este proyecto, FSEOM contaba con la empresa ******EMPRESA.1*** como proveedor y encargado del tratamiento de los datos personales recogidos en el marco del citado estudio.

Con fecha 23 de junio de 2023, se notificó a esta Agencia una brecha de datos personales por la FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA, con NIF G07324239.

En esta notificación se informaba de lo siguiente:

- El incidente ha sido Intencionado, para hacer daño al responsable / encargado o a las personas afectadas
- El origen del incidente ha sido: Externo: Otros, ajenos al responsable y encargado del tratamiento
- ¿Qué puede haber ocurrido?: Ciberincidente: ***(…)***
- Como consecuencia del incidente, se ha visto afectada la: Confidencialidad

- Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿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
- ¿Qué puede haber ocurrido? Puede seleccionar varias opciones: Ser víctima de campañas de phishing / spamming, Pérdidas financieras, Pérdida de control sobre sus datos personales
- ¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas? Las personas pueden encontrar inconvenientes importantes, produciendo un daño limitado, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)
- A fecha de esta notificación, ¿tiene constancia de que se hayan materializado alguno de los daños identificados, con el grado indicado en la cuestión anterior? No
- Como valora la probabilidad de que el daño anterior se materialice sobre las personas afectadas con la severidad indicada Alta
- Introduzca una breve descripción de lo ocurrido. El pasado miércoles, 14 de junio de 2023, a últimas horas de la tarde, ******EMPRESA.1*** detectó un acceso no autorizado ***(…)*** que afecta directamente a datos personales de participantes en un estudio promovido por la Sociedad Española de Oncología Médica, del que ******EMPRESA.1*** es la CRO y proveedor tecnológico y, además, encargado del tratamiento.
- Tipos de datos afectados: Datos de contacto, De salud (otros datos de salud)
- En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales? ***(…)***
- 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 20/06/2023
- ¿Conoce la fecha en la que se inició la brecha? Aproximadamente / Estimada
- Indique la fecha de inicio de la brecha 14/06/2023
- Medidas de seguridad antes de la brecha: ***(…)***
- ¿Ha adoptado tras el incidente nuevas medidas de seguridad que podrían haber evitado la brecha? Si
- Marque exclusivamente las nuevas medidas de seguridad y las que se hayan actualizado ***(…).***
- Comunicación a los afectados por la brecha de datos personales ¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas? No, pero serán informados
- A más tardar, las personas afectadas serán informadas en la siguiente fecha: 21/07/2023
- Medio por el que se informará Comunicación dirigida personalmente a cada afectado (postal, email, sms o similar), Comunicado público o publicación en web corporativa
- Encargado de tratamiento ¿Hay implicado un encargado de tratamiento en la brecha de datos personales? Si
- Nombre de la Organización ******EMPRESA.1.***

El 21 de julio de 2023 la FSEOM presentó ante esta Agencia un escrito de ampliación de notificación de esta brecha, en el que la información inicialmente proporcionada se mantenía intacta, a excepción de:

- ¿Cuál es su intención? Modificar una notificación hecha con anterioridad para proporcionar información relevante
- ¿Qué puede haber ocurrido? Puede seleccionar varias opciones: Ser víctima de campañas de phishing / spamming, Pérdida de control sobre sus datos personales
- ¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas? 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.)
- En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales? 2622
- Indique la fecha en la que se dio por resuelta la brecha 20/07/2023
- Comunicación a los afectados por la brecha de datos personales ¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas? Si
- Fecha en la que se informó: 20/07/2023
- Número de personas informadas 2622
- Medio por el que se ha informado Comunicación dirigida personalmente a cada afectado (postal, email, sms o similar) con garantía de entrega y lectura, Comunicado público o publicación en web corporativa

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 13 de julio de 2023, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

TERCERO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

El 12 de febrero de 2024 se recibió un escrito de la FSEOM, en respuesta a requerimiento de esta Agencia, en el que se aporta, entre otra, la siguiente información:

1. Se aporta como Documento núm. 1: Informe pericial de la brecha, con fecha 5 de julio de 2023, realizado por la Asociación Nacional de Ciberseguridad y Pericia Tecnológica, este informe incorpora las siguientes afirmaciones realizadas por el perito informático:

"(…)".

"*Recomendaciones técnicas que permitirían mejorar la plataforma del cliente:*
(…)

"En el transcurso del trabajo y redacción de este dictamen pericial, ******EMPRESA.1*** *ha implementado distintas mejoras sobre sus procedimientos, que expongo a continuación:*

(…)

"Además, he podido constatar la planificación de medidas técnicas de mejora que están en marcha o se iniciarán en breve:
(…)

El informe pericial concluye con el siguiente texto:

(…)

2. Se aporta como Documento núm. 2: informe pericial realizado por empresa externa contratada por FSEOM a raíz de la brecha (******EMPRESA.2***), de fecha 9 de febrero de 2024. De su contenido se destaca:

- *"Se notifica por parte de* ******EMPRESA.1*** *a SEOM … mediante correo electrónico fechado el 16 de junio, viernes a las 17:44, el incidente que fue detectado el día 14 de junio afectando a un número indeterminado de clientes de* ******EMPRESA.1****, entre ellos SEOM, indicando que con la información disponible no se puede concluir que exista afectación a datos personales (…)*
  El martes 20 de junio a las 17:44 se realiza una nueva comunicación por email desde ******EMPRESA.1*** *informando a SEOM de las medidas adoptadas en sus sistemas, así como del hecho de que no podían concluir aun fehacientemente que hubiese habido afectación a datos personales pero que era posible y lo confirmarían si hubiese sido así.*
  Por la información que obra en poder de ******EMPRESA.2****, la confirmación de la afectación de datos personales se produce el día 21 de junio, momento en el cual SEOM envía a* ******EMPRESA.1*** *formulario de notificación para poder comunicar el incidente de forma adecuada a la AEPD, el formulario se recibe el día 22 de junio. Se concluye que en el caso de SEOM, la afectación a los datos personales implica a unos* ***(…)*** *participantes del estudio observacional del proyecto* ******PROYECTO.1****."*

- *"En todo este proceso* ******EMPRESA.2*** *comenzó a dar apoyo a SEOM a partir del citado día 23 de junio finalizando el 19 de julio tras el análisis del informe pericial recibido por parte de* ******EMPRESA.1****.*
  El objetivo perseguido por SEOM era contrastar la veracidad de la información aportada por ******EMPRESA.1*** *y ampliar lo máximo posible la información para poder evaluar acciones a realizar. (…)*
  Tras la recepción del informe pericial realizado por ******EMPRESA.1*** *se trasladó el día 18 de julio, la valoración de* ******EMPRESA.2*** *al respecto, concluyendo que la información aportada por dicho informe era correcta y las medidas*

adoptadas igualmente adecuadas y evaluando que, en el momento de incidente:

- o ***(…)***

- *"Hemos de indicar que tras segundo análisis de la información recibida entre el 23 de junio y el 19 de julio de 2023, incluido algún documento posterior, estimamos que aunque la información de los sistemas y aplicativos centrales de* ******EMPRESA.1*** *es muy completa, así como las medidas implementadas también son satisfactorias, falta completar para SEOM información sobre* ***(…)*** *y que fue el vector origen del incidente, en concreto:*
  - ***(…)***"

3. Se afirma que "*Los datos personales afectados por el ciberataque y que se encontraban almacenados en los servidores de* ******EMPRESA.1*** *fueron los siguientes:*

- *Correo electrónico del participante en el Estudio Observacional*
- *Número de teléfono móvil*
- *Datos relativos a la salud (…) consistentes en:*
  - ⇨ ***(…)***

Se aporta como Documento núm. 3: los cuatro cuestionarios de recogida de datos, en los que se solicita, entre otra, la siguiente información: "***(…)"*** y preguntas relativas a la salud (***…)***.

4. Se aporta como Documento núm. 4: registro de actividades de tratamiento de la FSEOM, con, entre otro, el siguiente contenido:

- *"REFERENCIA: PROYECTO_* ******PROYECTO.1****"*
- *"Encargados de tratamiento": "*******EMPRESA.1****: CRO que gestiona el Estudio Observacional en su conjunto desde el punto de vista de la gestión del estudio observacional y desde el punto de vista tecnológico (APP móvil y arquitectura tecnológica)".*
- *"¿Cómo se produce?": "Recogida, almacenamiento, pseudonimización, extracción de datos pseudonimizados. Acceso a datos pseudonimizados".*
- *"¿Ha firmado contrato?": "Si".*

5. "*En relación con la comunicación realizada a los afectados informando de la brecha sufrida: con fecha 20 de julio de 2023 se realizó el envío del aviso de incidencia "INCIDENCIAI INFORMÁTICA ESTUDIO* ******PROYECTO.1****" a través de la plataforma* ******URL.1*** *a todos los participantes en el estudio "*******PROYECTO.1****" cuya extensión del texto es correspondiente a 4 SMS consecutivos con el siguiente tenor.*

"INCIDENCIA INFORMATICA ESTUDIO ******PROYECTO.1*** *Le informamos que se ha producido una incidencia informática en el almacenamiento de datos del estudio* ******PROYECTO.1,*** *en el que ha participado. La incidencia ya ha sido resuelta. Le recomendamos que haga caso omiso a cualquier comunicación vía móvil que no sea remitida por su hospital u oncólogo. Podrá acceder a la información completa sobre la incidencia y el alcance en relación con sus datos, a través del enlace seguro a nuestro servidor:* ******URL.2****".*

El enlace inserto en el SMS es la ruta a un archivo oculto y privado en el servidor de página web www.seom.org y que adjuntamos como DOCUMENTO NÚM.5"

Se aporta como Documento núm. 5 un documento titulado "COMUNICADO FSEOM ESTUDIO ******PROYECTO.1***" con, entre otro, el siguiente contenido:

"Desde la FUNDACION SOCIEDAD ESPAÑOLA DE ONCOLOGÍA MÉDICA (FSEOM) informamos de que le paso 14 de junio de 2023, el proveedor del estudio ******PROYECTO.1,*** *sufrió un ataque informático que ha afectado* ***(…)****, lo que ha supuesto una brecha de confidencialidad de algunos datos personales de los participantes.*

Como la privacidad es muy importante para nosotros, hemos tomado todas las medidas a nuestro alcance para solucionar el incidente y minimizar los daños que pudieran causarse; ***(…)****.*

Debido a ello, podría producirse cierta pérdida de control sobre los datos personales de los participantes, así como la recepción de comunicaciones no deseadas ***(…).*** *(…)"*

En su escrito de 12 de febrero de 2024, la FSEOM afirmó que: "*El aviso fue entregado correctamente al 84.4% (****(…)*** *usuarios) de los destinatarios y por el contrario no puedo entregarse al 15.6% (****(…)*** *usuarios). Se adjuntan informe de entrega y de envío por usuarios como DOCUMENTOS NÚM. 6. También se aporta copia de la notificación y del procedimiento de remisión como DOCUMENTOS NÚM. 7."*

Se aporta como Documento núm. 6 capturas de pantalla con el siguiente contenido:

"*Comunicado julio23*
Detalles
Fecha: 20/07/2023 13:10
Usuario: fseom
Destinatarios: ***(…)***
SMS/Destinatarios: 4
Total SMS: 10460
Coste: ***(…)*** *€"*

"Mensajes
Desconocidos: 0
Entregados: ***(…)***
No entregados: ***(…)****"*

El texto del mensaje enviado es el mismo que se reprodujo anteriormente.

Se aporta como Documento núm. 7 una planilla con los siguientes campos en la fila superior: "*Número", "Referencia", "Nombre", "Apellidos", "Entrega*" (columna completada con los valores "*Entregado"/"No entregado*"), "*SMS enviado", "SMS entregado*".

También se adjunta una planilla con los siguientes campos en su fila superior: "*Visita*" (columna completada con los valores "*no*" en todas sus filas), *"Clicks", "Ubicación", "Dispositivo", "Modelo", "Email", "Fecha de naci*".

Asimismo, se acompaña una planilla con los siguientes campos en su fila superior: "*Usuario", "Id SMS", "IdCampaña", "Referencia uso", "Fecha de enví", "Informe de en", "Fecha Informe", "Remitente", "Destinatario", "País", "Routing", "#SMS", "Mensaje", "Operadora", "CompatibleR", "En lista negra", "Descripción e", "Tipo de error", "Nombre campaña*".

6. Se aporta como Documento Núm. 8 un certificado firmado el 7 de febrero de 2024 por el secretario de FSEOM, en el que certifica: "*Que, tras la comunicación a los afectados de la brecha de seguridad de datos personales ocurrida el día 14 de junio del 2023, no hemos recibido ninguna reclamación o comunicación al respecto por parte de ninguno de ellos*."

7. Se aporta como Documento Núm. 9 captura de pantalla de un correo electrónico enviado el 20 de junio de 2023 desde ******EMPRESA.1*** a FSEOM con, entre otro, el siguiente contenido (sic):

"*Conforme a la conversación mantenida ayer, nos gustaría servirnos de este email para compartir con vosotros información más detallada acerca del incidente de seguridad sufrido por* ******EMPRESA.1*** *mediante un hackeo de un sistema secundario de almacenamiento. (…)*

Tras días de análisis, tanto por nuestro equipo interno, como por asesores externos y un peritaje tecnológico, vamos conociendo más información acerca de lo ocurrido y, en este momento, no podemos definitivamente confirmar que, en vuestro caso, se hayan visto afectados datos personales relativos a la salud de los pacientes. (…)".

También se aporta captura de pantalla de un correo electrónico enviado el 16 de junio de 2023 desde ******EMPRESA.1*** a FSEOM con, entre otro, el siguiente contenido:

"Estimado Cliente,
*Nos ponemos en contacto con Usted para comunicarle, de manera fehaciente, que desde ***EMPRESA.1 se ha detectado un acceso no autorizado a un sistema secundario de almacenamiento que afecta directamente a los datos personales alojados en una base de datos de la cual Usted es Responsable o Encargado del Tratamiento. (…)*

(i) Fecha en la que se ha detectado la brecha de seguridad: En la tarde del Miércoles 14 de junio de 2023
(ii) *Naturaleza de la violación: Acceso no consentido a* ***(…)****.*
(iii) *Proyectos afectados:* ******PROYECTO.1***
(iv) *Número potencial de datos afectados:* ***(…)***
(v) Categorías de datos afectados:
- ***(…)****"*

8. En su escrito de 12 de febrero de 2024 FSEOM indicó: "*Se adjunta como DOCUMENTO NÚM. 10" el Contrato de Prestación del Servicio y el Contrato de*

Encargado de Tratamiento suscrito entre FSEOM y ******EMPRESA.1****. Adicionalmente,* ******EMPRESA.1*** *relleno un check list que certificaba si era un proveedor compliance in privacy, documento que también se adjunta a este bloque documental" (sic)*.

Se aporta como Documento núm. 10 copia de contrato de fecha 20 de abril de 2021 entre ******EMPRESA.1*** (como proveedor) y FSEOM (como cliente), para la realización del proyecto "******PROYECTO.1***".

También se aporta copia de contrato entre FSEOM y ******EMPRESA.1***, con el objeto de "*definir las condiciones conforme a las cuales el ENCARGADO DEL TRATAMIENTO llevará a cabo el tratamiento de datos personales para la prestación del servicio contratado por FSEOM, de conformidad con lo dispuesto en la legislación española de protección de datos y en el artículo 28 del RGPD y concordantes*".

En el punto 3 del contrato se establece: "*El encargado deberá adoptar las medidas que a tenor del análisis de riesgos realizado por FSEOM, se le hayan comunicado y resulten necesarias para garantizar un nivel adecuado de seguridad, tales medidas se facilitan en el anexo II de este contrato*".

Del Anexo II destacan las siguientes medidas (entre otras):

"***(…)***".

El contrato también incorpora un apéndice (*Apéndice 3)* con información adicional sobre las Medidas de Seguridad de ******EMPRESA.1***, destacando las siguientes como relevantes:

"***(…)***"

9. Se aporta como Documento núm. 11 documento de "Informe de riesgos para los derechos y libertades y EIPD" de fecha 25 de junio de 2021 con, entre otro, el siguiente contenido:

- "*ACTIVOS DE SOPORTE UTILIZADOS*
  Los activos de soporte que se precisa para la realización de las operaciones de tratamiento prevista son:
    - ***(…)***

- "*El flujo de datos será el siguiente:*
  (…)

- *"Las operaciones de tratamiento que se pretenden abordar por parte de la entidad suponen un alto riesgo ara los derechos y libertades de los interesados derivados de:*
    - *Tratamiento de datos especialmente sensibles, relacionados con la salud del participante del Estudio Observacional (artículo 9 del RGPD)" (sic)*

- "*Para el tratamiento de los datos personales cuyo riesgo es la revelación de categorías especiales de datos que producen efectos jurídicos sobre las*

personas tales como: discriminación, pérdida de control por el responsable o pérdida de control del secreto profesional, se han propuesto los siguientes controles:

- ***(…)***
-

(…) En relación con la revelación de datos de especial categoría, el nivel de riesgo residual es medio."

- En cuanto al responsable de la implementación de tales medidas, el documento señala a "******PUESTO.1 e ***EMPRESA.1***".

10. Se aporta como Documento núm. 12 un documento de ******EMPRESA.1*** con el título "NUEVAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADOPTADAS POR ******EMPRESA.1*** PARA EVITAR, EN LO POSIBLE, INCIDENTES DE SEGURIDAD COMO EL SUCEDIDO". De su análisis se extraen, entre otras, las siguientes afirmaciones (el subrayado es nuestro):

- ***"(…)***

11. Se aporta como Documento núm. 13 un documento de ***EMPRESA.1 con el título "MEDIDAS DE SEGURIDAD PARA REDUCIR RIESGO A ATAQUE SIMILAR" con las medidas que se llevaron a cabo para reducir el riesgo de un ataque de similares características. De su análisis se extraen, entre otras, las siguientes afirmaciones:

(…)

12. Se aporta como Documento núm. 14 un documento de FSEOM con el título "Procedimiento de respuesta a brechas de seguridad", en el que, entre otra información, se indica:

"*Este procedimiento establece los siguientes aspectos:*

- *Roles y responsabilidades del personal.*
- *Detalles de los contactos adecuados.*
- *Canal de comunicación adecuado.*
- *Pasos que seguir*."

También se aporta un documento de ******EMPRESA.1*** con el título "Notificación y comunicación de incidentes" (original en inglés).

13. Se aporta como Documento núm. 15 una factura de ******EMPRESA.2*** a FSEOM, de fecha 26 de junio de 2023, con la siguiente referencia "******REFERENCIA.1***".

También se aportan tres facturas de ******EMPRESA.5*** a FSEOM, de fecha 13 de septiembre de 2023, en concepto de: "***(…)***

14. Se aporta como Documento núm. 16 copia de denuncia presentada ante la Policía Nacional el 17 de junio de 2023 por el representante de ******EMPRESA.1***, quien denunció que:

"--…ha habido un acceso no autorizado ***(…)****.*

*-- Se localiza en el servidor un archivo virtual txt cuyo contenido es el siguiente: "Contact *****EMAIL.1** or *****EMAIL.2** ASAP to recovery. Your files are safe".*

También se aporta copia de denuncia presentada ante la Policía Nacional el 12 de julio de 2023 por el representante de FSEOM, quien denunció que:

*"—Que el día 19 de junio del presente año, se informa a la Fundación de que los servidores contratados por *****EMPRESA.1** han sufrido un ciberataque resultando sustraídos los datos de los pacientes que participaron en el estudio anteriormente señalado".*

15. Indica FSEOM que "Se adjunta como DOCUMENTO NÚM. 17, copia de la formación realizada en FSEOM en materia de incidentes de seguridad, y copia del argumentario preparado para atender a aquellos afectados de la brecha de seguridad para el caso de que contactasen con FSEOM (DOCUMENTO NÚM. 18).

Se aporta como Documento Núm. 17 un documento de "******REFERENCIA.2***" con el título "Planificación e implantación de procesos para detectar, contener y mitigar una Violación de Seguridad".

Se aporta como Documento Núm. 18 un documento de "******REFERENCIA.3***" con el título "Argumentario (Q&A)", en el que se indica:

"(…) ¿Qué ocurre si utilizan fraudulentamente mis datos? ¿Qué riesgos corro?
Son varios los usos fraudulentos de los datos obtenidos por procedimiento delictivo. Lo común es la venta a empresas comercializadoras, así como intentos de acceso a los dispositivos personales.
*En el caso de venta de datos a empresas comercializadoras, el efecto será la recepción de publicidad no deseada por diferentes vías, **(…).***
Los mayores riesgos están en relación con intentos de acceso a los dispositivos y a la información contenida en ellos (datos personales, cuentas bancarias, etc.), así como la suplantación de identidad (…)".

16. En su documento de 12 de febrero de 2024, FSEOM indica: "6.4.- En relación con la aclaración referida a que la brecha se hubiera podido evitar adoptando alguna medida adicional, nos referimos a que si ******EMPRESA.1*** hubiera dado cumplimiento a la medida ***(…)*** acordada en contrato, se hubiera podido evitar el impacto a los afectados." (sic)

Por su parte, en el marco de las actuaciones previas de investigación, esta Agencia ha realizado una serie de comprobaciones en Internet:

- El 11 de septiembre de 2024 esta Agencia comprobó que, en relación con la medida reactiva implantada de sustitución de tokens por roles, en la propia web de ******APP.1*** con título "*Mejores Prácticas de Seguridad Recomendadas Por *****APP.1***", se incorporaba el siguiente texto extraído de la documentación oficial de ******APP.1***, en el que se recomendaba no utilizar las claves de acceso de forma directa en la aplicación que necesita acceder a recursos de *****EMPRESA.3** (tokens programáticos), utilizando en su lugar los ROLES como buena práctica de seguridad (******URL.3***):

> *"Uso de roles de ***APP.3 para Aplicaciones y Servicios de *****APP.1** que requieren acceso a *****EMPRESA.3**:*
> *Para que las aplicaciones que se ejecutan en *****EMPRESA.4** u otros Servicios de *****APP.1** accedan a recursos de *****EMPRESA.3**, deben incluir credenciales de *****APP.1** válidas en sus solicitudes a la API de *****APP.1**. Recomendamos no almacenar las credenciales de *****APP.1** de forma directa en la aplicación ni en una instancia de *****EMPRESA.4**. Estas son las credenciales a largo plazo que no rotan automáticamente y que podrían tener un impacto empresarial significativo si se comprometen.*
> *En su lugar, utilice un ROL de ***APP.3 para administrar temporalmente las credenciales para las aplicaciones o los servicios que necesiten acceder a *****EMPRESA.3**. Cuando utiliza un ROL, no tiene que distribuir credenciales a largo plazo (como un nombre de usuario y una contraseña o claves de acceso) a una instancia de *****EMPRESA.4** o un servicio de Servicio de *****APP.1** como *****APP.2**. El ROL proporciona permisos temporales que las aplicaciones pueden utilizar cuando hacen llamadas a otros recursos de *****APP.1**."*

- El 19 de septiembre de 2024 esta Agencia comprobó que, con respecto a los procesos establecidos en la norma ISO 27001, en el *Anexo A.10* de esta norma, que establece los controles criptográficos para proteger la información, requisitos de cifrado de los datos especialmente protegidos, se indica: "*Los controles criptográficos del Anexo A.10 se basan en el principio del mínimo privilegio y exigen que sólo las personas autorizadas tengan acceso a las claves criptográficas y que estas claves estén debidamente protegidas*."

- El 20 de septiembre de 2024 esta Agencia comprobó que, en la documentación oficial de *****APP.1**, en relación con la "*Administración de Identidades*" y *"Las mejoras prácticas para almacenar y usar secretos de forma segura" en el enlace* *****URL.4** podía verse el siguiente contenido, entre otro (el subrayado es nuestro):

> *"Un antipatrón común es incrustar claves de acceso de *****APP.3** dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se requiera una clave de acceso de *****APP.3** para comunicarse con un servicio de *****APP.1**, utilice credenciales de seguridad temporales (a corto plazo).*
> *Estas credenciales a corto plazo pueden proporcionarse a través de roles de *****APP.3** para instancias de **(...)**, roles de ejecución para funciones *****APP.4**, roles de *****APP.3** de *****EMPRESA.6** para el acceso de usuarios móviles y políticas de *****APP.5** para dispositivos IoT.*
> *Cuando interactúe con terceros, es preferible que delegue el acceso a un rol de *****APP.3** con el acceso necesario a los recursos de su cuenta en lugar de configurar un usuario de *****APP.3** y enviar a ese tercero la clave de acceso secreta para ese usuario."*

- El 24 de septiembre de 2024 esta Agencia comprobó que en la documentación oficial de ******APP.1***, en relación con la información sobre buenas prácticas en seguridad y recomendaciones para la implementación del Esquema Nacional Nivel MEDIO a través de la configuración de ******APP.1***, en la página web ******URL.5*** podía verse, entre otro, el siguiente contenido (La información no estaba actualizada con la última versión del ENS (RD 311/2022):

  > *Medida relacionada del RD 3/2010 (Anexo II 4.2.5. Mecanismo de Autenticación, página 27):*
  > "*El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de* ******APP.3****. Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de* ******APP.1*** *para ayudar a incorporar el principio de funcionalidad mínima*".

CUARTO: De acuerdo con el informe recogido de la herramienta AXESOR el 15 de diciembre de 2024, la entidad FSEOM es una asociación con un volumen de ventas de ***(…)*** euros.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

II
Procedimiento

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos".*

De acuerdo con el artículo 64 de la LOPDGDD, y teniendo en cuenta las características de la presunta infracción cometida, se inicia un procedimiento sancionador.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en

consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

III
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que FSEOM realiza, entre otros tratamientos, la recogida y conservación de datos personales de personas físicas: correo electrónico, número de teléfono móvil y datos relativos a la salud.

FUNDACION SEOM realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

IV
Obligación incumplida. Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

Pérdida de confidencialidad de los datos personales

El 23 de junio de 2023, FSEOM, en su calidad de responsable del tratamiento, notificó a esta Agencia una brecha de datos personales en la que informaba que "******EMPRESA.1*** detectó un acceso no autorizado ***(…)*** que afecta directamente a datos personales de participantes en un estudio promovido por la Sociedad Española de Oncología Médica, del que ******EMPRESA.1*** es la CRO y proveedor tecnológico y, además, encargado del tratamiento".

En su escrito de 12 de febrero de 2024, FSEOM aporta como Documento núm. 10 la copia de contrato de fecha 20 de abril de 2021 entre ******EMPRESA.1*** (como proveedor) y FSEOM (como cliente), para la realización del proyecto "******PROYECTO.1***".

Por todo lo expuesto, esta Agencia entiende que se habría producido una pérdida de confidencialidad de los datos personales vinculados proyecto "******PROYECTO.1*** promovido por FSEOM***.***

Datos personales afectados

El 21 de julio de 2023 la FSEOM presentó ante esta Agencia un escrito de ampliación de notificación de esta brecha, en el que indicaba que se habían visto afectados por este incidente los datos de contacto y de salud de ***(…)*** personas.

En su escrito de 12 de febrero de 2024 FSEOM indicó que "*Los datos personales afectados por el ciberataque y que se encontraban almacenados en los servidores de* ******EMPRESA.1*** *fueron los siguientes:*

- *Correo electrónico del participante en el Estudio Observacional*
- *Número de teléfono móvil*
- *Datos relativos a la salud (…) consistentes en:*
  - ⇨ ***(…)***

En el Documento núm 3 de tal escrito puede verse que se solicitaba a los interesados los siguientes datos personales: "***(…)"*** y preguntas relativas a la salud (***…)***.

Por todo lo expuesto, esta Agencia entiende que se habrían visto afectados por la brecha objeto del presente procedimiento los siguientes datos personales de ***(…)*** personas físicas: ***(…)*** y preguntas relativas a la salud.

Cronología de los hechos y medidas técnicas u organizativas

El 20 de abril de 2021 según se desprende del Documento núm. 10 anexo al escrito de FSEOM de 12 de febrero de 2024, FSEOM y ***EMPRESA.1 firmaron un contrato de encargado de tratamiento, en cuyo Anexo II se obligaba a ***EMPRESA.1 a "***(…)***".

También este contrato incorporaba un Apéndice 3 con información adicional sobre las Medidas de Seguridad de ******EMPRESA.1***, entre las que se contaba:

(…).

El 23 de junio de 2023, FSEOM, en su calidad de responsable del tratamiento, notificó a esta Agencia una brecha de datos personales en la que informaba que ******EMPRESA.1*** (encargado del tratamiento) detectó un acceso no autorizado a los datos personales de participantes en el estudio del proyecto "******PROYECTO.1***".

El 5 de julio de 2023 la Asociación Nacional de Ciberseguridad y Pericia Tecnológica realizó un informe del incidente en el que indicaba que el 14 de junio de 2023 ******EMPRESA.1*** detectó ***(…).***

El informe explicaba que ***(…).***

En cuanto a la cronología de los hechos, ***(…).***

El ataque se produjo por ***(…)."***

El citado informe pericial enumera una serie de recomendaciones técnicas para mejorar la plataforma de ***EMPRESA.1**, entre las que destacan: ***(…)***.

También en el informe se detallan mejoras implementadas por ***EMPRESA.1**, respecto a ***(…).***

El 9 de febrero de 2024 la empresa ***EMPRESA.2** realizó un segundo informe pericial de la brecha en cuestión, en el que se indicaba que en el momento del incidente ***(…)***.

EMPRESA.1 habría implantado "NUEVAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADOPTADAS POR ***EMPRESA.1** PARA EVITAR, EN LO POSIBLE, INCIDENTES DE SEGURIDAD COMO EL SUCEDIDO", tales como: ***(…),
También ***EMPRESA.1 habría adoptado "MEDIDAS DE SEGURIDAD PARA REDUCIR RIESGO A ATAQUE SIMILAR" como:

(…)

Por su parte, el 11 de septiembre de 2024 esta Agencia comprobó que, en relación con la medida reactiva implantada de sustitución de tokens por roles, en la propia web de ***APP.1** con título "*Mejores Prácticas de Seguridad Recomendadas Por ***APP.1**"*, se incorpora el siguiente texto extraído de la documentación oficial de ***APP.1***, en el que se ***(…).***

El 19 de septiembre de 2024 esta Agencia comprobó que, con respecto a los procesos establecidos en la norma ISO 27001, en el *Anexo A.10* de esta norma, que establece los controles criptográficos para proteger la información, requisitos de cifrado de los datos especialmente protegidos, se indica: "*Los controles criptográficos del Anexo A.10 se basan en el principio del mínimo privilegio y exigen que sólo las personas autorizadas tengan acceso a las claves criptográficas y que estas claves estén debidamente protegidas*."

El 20 de septiembre de 2024 esta Agencia comprobó que en la documentación oficial de ***APP.1***, en relación con la "*Administración de Identidades*" y *"Las mejoras prácticas para almacenar y usar secretos de forma segura" en el enlace* ***URL.4*** puede verse el siguiente contenido, entre otro (el subrayado es nuestro):

> *"Un antipatrón común es incrustar claves de acceso de ***APP.3** dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se requiera una clave de acceso de ***APP.3** para comunicarse con un servicio de ***APP.1**, utilice credenciales de seguridad temporales (a corto plazo).*
> *Estas credenciales a corto plazo pueden proporcionarse a través de roles de ***APP.3** para instancias de **(...)**, roles de ejecución para funciones ***APP.4**, roles de ***APP.3** de ***EMPRESA.6** para el acceso de usuarios móviles y políticas de ***APP.5** para dispositivos IoT.*
> *Cuando interactúe con terceros, es preferible que delegue el acceso a un rol de ***APP.3** con el acceso necesario a los recursos de su cuenta*

> *en lugar de configurar un usuario de *****APP.3** y enviar a ese tercero la clave de acceso secreta para ese usuario."*

El 24 de septiembre de 2024 esta Agencia comprobó que en la documentación oficial de ******APP.1***, en relación con la información sobre buenas prácticas en seguridad y recomendaciones para la implementación del Esquema Nacional Nivel MEDIO a través de la configuración de ******APP.1***, en la página web ******URL.5*** puede verse, entre otro, el siguiente contenido (La información no está actualizada con la última versión del ENS (RD 311/2022):

> *Medida relacionada del RD 3/2010 (Anexo II 4.2.5. Mecanismo de Autenticación, página 27):*
> "*El acceso a los sistemas y activos se puede controlar comprobando que el usuario raíz no tenga claves de acceso adjuntas a su función de *****APP.3**. Asegúrese de eliminar las claves de acceso raíz. En su lugar, cree y utilice el sistema basado en roles Cuentas de *****APP.1** para ayudar a incorporar el principio de funcionalidad mínima*".

En conclusión, el hecho de que ******EMPRESA.1*** (encargado del tratamiento) no tuviera implantadas las medidas que han sido examinadas, facilitó que la brecha de datos personales se produjera y el mayor impacto de la misma. Las referidas medidas fueron introducidas por el encargado el tratamiento a posteriori (de forma reactiva), con el fin de evitar que volviera a producirse una brecha de datos personales similar.

En virtud del artículo 4.8 del RGPD el encargado del tratamiento es quien "*trate datos personales por cuenta del responsable del tratamiento*".

Aunque la brecha de datos personales se produjera en los sistemas de ******EMPRESA.1***, encargado del tratamiento, y aunque dicho encargado no tuviera implantadas, en el momento en el que se produjo la brecha de datos personales las medidas que acaban de ser analizadas, que, con gran probabilidad, habrían impedido que dicha brecha se produjera o, al menos, habrían reducido su impacto, el responsable del tratamiento es FSEOM.

Por todo lo expuesto, esta Agencia entiende que FSEOM, como responsable del tratamiento, no tenía implantadas las medidas técnicas u organizativas apropiadas para evitar un incidente como el que se produjo.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a FSEOM, por vulneración del artículo 5.1.f) del RGPD.

V
Tipificación de la infracción del artículo 5.1.f) del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de

una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679."

VI
Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
*i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas prev***APP.3ente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de ventas de FSEOM (***(…)*** euros).

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de

acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2, letra a), del RGPD): por el acceso indebido a los datos personales de ***(…)*** personas físicas: ***(…)***, debido a no contar con las medidas técnicas u organizativas apropiadas para evitar un incidente como el que dio origen al presente procedimiento.
- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): Entre los datos afectados por la brecha, había datos de salud de los pacientes participantes en el Proyecto "******PROYECTO.1***".

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD): FSEOM se trata de una organización dedicada a recabar datos de salud sobre una patología determinada, por lo que está habituada al tratamiento de datos personales

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar inicialmente una sanción de multa administrativa de 70.000,00 euros.

VII
Medidas correctivas

De confirmarse la infracción, la resolución que se dicte podrá establecer las medidas correctivas que la entidad infractora deberá adoptar para poner fin al incumplimiento de la legislación de protección de datos personales, en este caso del Artículo 5.1.f) del RGPD, de acuerdo con lo establecido en el citado artículo 58.2.d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…"*

Así, se podrá requerir a la entidad responsable para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En el presente acto se establece cuál es la presunta infracción cometida y los hechos que podrían dar lugar a esa posible vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

No obstante, en este caso, con independencia de lo anterior, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, en la resolución que se adopte se podrá requerir a FUNDACION SEOM para que, en el plazo de TRES MESES, a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Acreditar la aplicación efectiva de las medidas técnicas y organizativas adecuadas, no solo para cumplir con la normativa, sino para demostrar su cumplimiento antes las autoridades de control e interesados.

La imposición de estas medidas es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Asimismo, se recuerda que ni el reconocimiento de la infracción cometida ni, en su caso, el pago voluntario de las cuantías propuestas, eximen de la obligación de adoptar las medidas pertinentes para que cese la conducta o se corrijan los efectos de la infracción cometida y la de acreditar ante esta AEPD el cumplimiento de esa obligación.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a **FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA**, con NIF **G07324239**, por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: NOMBRAR como instructor/a a ***R.R.R.*** y, como secretario/a, a ***S.S.S.***, indicando que podrán ser recusados, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente, a efectos probatorios, la notificación de la violación de la seguridad de los datos personales, así como, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de 70.000,00 euros, sin perjuicio de lo que resulte de la instrucción.

QUINTO: NOTIFICAR el presente acuerdo a FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA, con NIF G07324239, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **56.000,00** euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **56.000,00** euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **42.000,00 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia expresos de cualquier acción o recurso en vía administrativa contra la sanción.

A estos efectos, en caso de acogerse a alguna de ellas, deberá remitir a la Subdirección General de Inspección de datos comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción indicando a cuál de las dos reducciones se acoge o si es a las dos.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente **(56.000,00** euros o **42.000,00 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000***

(BIC/Código SWIFT: CAIXESBBXXX) abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección junto con la comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción para continuar con el procedimiento en concordancia con la cantidad ingresada.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

1479-111224

Mar España Martí
Directora de la Agencia Española de Protección de Datos

>>

SEGUNDO**:** En fecha 15 de enero de 2025, ***FSOM*** ha procedido al pago de la sanción en la cuantía de **42.000,00 euros** haciendo uso de las dos reducciones previstas en el acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad en relación con los hechos a los que se refiere el acuerdo de inicio y su calificación jurídica.

TERCERO**:** ***FSOM*** ha renunciado expresamente a cualquier acción o recurso en vía administrativa contra la sanción.

CUARTO: En el acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá “ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…”.

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

*El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentar***APP.3ente."*

III
Pago voluntario y reconocimiento de responsabilidad

De conformidad con lo dispuesto en el citado artículo 85 de la LPACAP, en el acuerdo de inicio notificado se informaba sobre la posibilidad de reconocer la responsabilidad y de realizar el pago voluntario de la sanción propuesta, lo que supondría dos reducciones acumulables de un 20% cada una. Con la aplicación de estas dos reducciones, la sanción quedaría establecida en **42.000,00 euros** y su pago implicaría

la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Tras la notificación del citado acuerdo de inicio, ***FSOM*** ha procedido al reconocimiento de la responsabilidad y al pago voluntario de la sanción, acogiéndose a las dos reducciones previstas y renunciando expresamente a cualquier acción o recurso en vía administrativa.

Debe tenerse en cuenta que, de acuerdo con los preceptos de la LPACAP, así como de la jurisprudencia del Tribunal Supremo en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Presidencia de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la comisión de las infracciones y CONFIRMAR las sanciones determinadas en la parte dispositiva del acuerdo de inicio transcrito en la presente resolución.

La suma de las citadas cuantías arroja una cantidad total **70.000,00 euros.**

Tras haber procedido ***FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA*** al pronto pago y reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPACAP, a la reducción de un 40% del total mencionado, lo cual supone la cantidad definitiva de **42.000,00 euros**.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202416691**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA*** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del acuerdo de inicio transcrito en la presente resolución.

CUARTO: NOTIFICAR la presente resolución a ***FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA***.

QUINTO: De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario y reconocimiento de la responsabilidad al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, por parte de la presente autoridad se acepta la renuncia expresamente manifestada por ***FUNDACIÓN SOCIEDAD CIENTÍFICA DE ONCOLOGÍA MÉDICA***, no cabiendo en consecuencia la interposición de recurso potestativo de reposición frente a la presente resolución, todo

ello sin perjuicio de la posibilidad de acudir a la vía jurisdiccional contencioso-administrativa.

En consecuencia, teniendo en cuenta lo dispuesto en el artículo 90 de la LPACAP, dado que no cabe ningún recurso en vía administrativa al haber renunciado expresamente, la presente resolución será firme y plenamente ejecutiva a partir de su notificación.

No obstante, conforme a lo previsto en el artículo 90.3.a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

1259-180225

Olga Pérez Sanjuán
La Subdirectora General de Inspección de Datos, de conformidad con el art. 48.2 LOPDGDD, por vacancia del cargo de Presidencia y Adjuntía