- **Expediente N.º: EXP202310012**

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 ***GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)*** (en adelante, ***GETECCU***), mediante el acuerdo que se transcribe:

<<
Expediente N.º: EXP202310012

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

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

Contenido

HECHOS

PRIMERO: Con fecha 19 de junio de 2023, el GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU), con NIF **G07762669** (en adelante, GETECCU) notificó a esta Agencia una brecha de datos personales.

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: Acceso no autorizado a datos en sistema de información (corporativo o servicio en internet)*
- *Como consecuencia del incidente, se ha visto afectada la: Confidencialidad*

- *Introduzca una breve descripción de lo ocurrido. "Acceso no consentido a archivos del sistema de almacenamiento secundario con borrado y posible descarga de los mismos."*
- *Tipos de datos afectados:* ***(…)***
- *Las personas afectadas tienen los siguientes perfiles:* ***(…)***
- *En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales?* ***(…)***
- *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 16/06/2023*
- *Fecha de inicio de la brecha 14/06/2023*
- *Medidas de seguridad antes de la brecha* ***(…)***
- Se identifica a GETECCU como responsable del tratamiento y a ******EMPRESA.1*** como encargado del tratamiento implicado en la brecha

El 11 de julio de 2023 GETECCU 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:

- *¿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.)*
- *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 Improbable*
- *Tipos de datos afectados* ***(…)***
- *En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales?* ***(…)***
- *¿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* ***(…).***
- *Indique la fecha en la que se dio por resuelta la brecha 10/07/2023*
- *¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas? No serán informados*
- *Las personas afectadas no serán informadas porque: La comunicación supone un esfuerzo excesivo*

Junto a esta segunda notificación se aporta:

- Informe pericial de la brecha, con fecha 5 de julio de 2023, realizado por la ******ORGANISMO.1***, 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:

(…)

SEGUNDO: En fecha 5 de julio de 2023 se recibió notificación de brecha de datos personales por parte del ***CENTRO.54 (en adelante, ***CENTRO.54), con la siguiente información:

- *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: Acceso no autorizado a datos en sistema de información (corporativo o servicio en internet)*
- *Como consecuencia del incidente, se ha visto afectada la: Confidencialidad*
- *Introduzca una breve descripción de lo ocurrido. "Estamos evaluando la brecha de seguridad que nos ha notificado GETECCU (Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa), encargado de tratamiento del proyecto *****PROYECTO.1** a través de su empresa contratada *****EMPRESA.1**., en parte de la infraestructura gestionada por ellos y que según indican afectan a datos personales y datos clínicos de (...) de los hospitales participantes en el proyecto ***PROYECTO.1, entre ellos el Hospital Universitario de Navarra. La brecha ya ha sido notificada por GETECCU a la AEPD y su número de registro es *****REFERENCIA.1**. Nos remitimos a los datos indicados en ese registro. El alcance global parece ser de unos **(…)** (...) a nivel estatal y unos **(…)** en Navarra. Según indican ya han notificado a medios judiciales y policiales. Nos han notificado que están trabajando en actualizar las medidas técnicas y organizativas de su organización en el marco del proyecto *****PROYECTO.1**. Además en el caso del ***CENTRO.54, estamos recabando la información para determinar el alcance y el impacto sobre los datos de nuestros (...) y evaluando y ampliando las medidas organizativas de nuestra organización."*

- *Tipos de datos afectados: Datos básicos (Ej: nombre, apellidos, fecha de nacimiento), Datos de contacto, De salud (otros datos de salud)*
- *Las personas afectadas tienen los siguientes perfiles: (...)*
- *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 04/07/2023*
- *Indique la fecha de inicio de la brecha 14/06/2023*
- *Medidas de seguridad antes de la brecha:* ***(…)***
- Se identifica el ***CENTRO.54 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha

En fecha 9 de agosto de 2023, se recibió en esta Agencia un escrito con, entre otro, el siguiente contenido:

"*La empresa GETECCU ha realizado ya la comunicación definitiva y finalizadora del proceso de información sobre la brecha de seguridad a la AEPD, en el que adjuntan el informe pericial final realizado para* ******EMPRESA.1*** *y que incluye las causas y las medidas implementadas, con el objetivo de mejorar la plataforma y prevenir futuros ataques que comprometan la seguridad.*
GETECCU, una vez analizado y valorado el nivel de riesgo, concluyendo que la comunicación a los (...) afectados supondría un esfuerzo desproporcionado, y en cumplimiento del artículo 34.d del Reglamento (UE) 2016/679, ha decidido adoptar las siguientes comunicaciones:
Comunicación de la brecha a los centros hospitalarios, Investigador Principal, y DPD.
Comunicación de los (...) afectados a aquellos Centros Hospitalarios que lo soliciten.
Comunicación de la brecha en la web https: geteccu.org
*Desde la Sección de Seguridad del ***CENTRO.54 entendemos que GETECCU ha cumplido con las obligaciones de comunicación a la AEPD y a los (...) afectados, y no disponemos de información adicional para aportar al caso."*

Con fecha 10 de agosto de 2023 tuvo entrada en esta Agencia una ampliación de información de la brecha notificada previamente por el ***CENTRO.54, en el que la información inicialmente proporcionada se mantenía intacta, a excepción de (entre otra):

- *¿Qué puede haber ocurrido? Puede seleccionar varias opciones: Pérdida de confidencialidad de datos afectados por secreto profesional, 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 Baja*
- *Introduzca una breve descripción de lo ocurrido. "La presente notificación es complementaria y finalizadora de la inicial. El ***CENTRO.54, como responsable del tratamiento, no tiene información adicional que complemente a la presentada por la empresa encargada del tratamiento."*
- *En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales? (...)*
- *Indique la fecha en la que se dio por resuelta la brecha 11/07/2023*
- *¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas? Si*
- *Fecha en la que se informó: 11/07/2023*
- *Número de personas informadas (...)*
- *Medio por el que se ha informado Comunicado público o publicación en web corporativa*
- Se identifica el ***CENTRO.54 como responsable del tratamiento y a ***EMPRESA.1** como encargado del tratamiento implicado en la brecha

TERCERO: Con fecha 4 de julio de 2023 la Autoridad Catalana de Protección de Datos (APDCAT) contactó con esta Agencia con motivo de haber recibido varias notificaciones de brecha de hospitales públicos catalanes dentro del ámbito de su competencia que identifican como encargado del tratamiento a GETECCU y subencargado del tratamiento a ***EMPRESA.1** APDCAT consultaba si GETECCU había notificado la brecha a la AEPD y con qué rol de protección de datos se identificaba para determinar a quien correspondería la obligación de comunicar a los afectados conforme al art. 34 del RGPD si fuera necesario.

La APDCAT remitió a esta Agencia por correo electrónico documentos facilitados por los hospitales que le habían notificado la brecha y que en resumen indicaban que la brecha habría afectado al llamado *****PROYECTO.1)**.

Se adjuntaba un documento con el título "PROYECTO ***PROYECTO.1**, con, entre otro, el siguiente contenido:

*"El objetivo global del proyecto *****PROYECTO.1** es la creación de una infraestructura y de los procedimientos operativos necesarios para el desarrollo continuado de estudios multicéntricos de colaboración en torno a los factores implicados en la etiología y fisiopatología de la enfermedad inflamatoria intestinal, incluyendo factores genéticos y ambientales, y estudios epidemiológicos"*

"Cada centro completará los formularios donde se incluye toda la información clínica de los (...) que se considera relevante para el desarrollo de los estudios. Esta información será actualizada periódicamente por los investigadores que sigan a los (...)."

*"Con el fin de facilitar la recogida de información clínica y genética y para proteger la privacidad de los (...), la información estará recogida bajo códigos de identificación. Los códigos de identificación serán generados por el programa de la base de datos de forma automática. Las muestras de sangre/ADN estarán marcadas con el código específico del proyecto *****PROYECTO.1**.*

La información clínica de cada paciente deberá contener una ficha con los datos completos de filiación del paciente, que se relacionará con un código del proyecto ******PROYECTO.1****. El acceso a la relación entre los datos de filiación y el código del proyecto* ******PROYECTO.1*** *será sólo accesible al médico responsable del paciente que generó la información, de forma que pueda identificar al paciente y comunicarle los resultados en caso de que lo estime necesario por el motivo que fuere, incluyendo la voluntad del paciente y el mejor tratamiento.*

Los investigadores tendrán sólo acceso a los códigos con su correspondiente información clínica asociada, y a las muestras de ADN codificadas en el caso de estudios genéticos."

"La información clínica de todos los (...) será recogida en una base de datos común del proyecto ******PROYECTO.1****. La información clínica recogida en el proyecto* ******PROYECTO.1*** *incluye datos de filiación del paciente, características de su enfermedad inflamatoria intestinal, exploraciones para la detección precoz de lesiones neoplásicas, tratamientos recibidos, respuesta a los mismos y efectos adversos asociados, visitas ambulatorias, hospitalizaciones, operaciones quirúrgicas y complicaciones de las mismas, factores de*
riesgo para el desarrollo de la enfermedad, incluyendo antecedentes familiares, comorbilidades asociadas e información sobre los descendientes.

Los investigadores participantes tendrán acceso integral a la información generada en centro, incluyendo los datos de identificación de los (...).

Los investigadores responsables de un estudio concreto tendrán acceso a la información de los (...) incluidos en el estudio particular contenida en la base de datos general y convenientemente anonimizada, en la que los casos serán solamente identificados mediante el código ******PROYECTO.1****."*

"El proyecto ******PROYECTO.1*** *se constituye en torno al Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU), quien nombrará al comité responsable del proyecto* ******PROYECTO.1*** *y estará compuesto por un número impar de miembros que a criterio de GETECCU se establecerá en 5 ó 7.*

El propietario, responsable de la base de dados y tratamiento de los datos es GETECCU.

GETECCU actuará como sociedad ante la que puedan ejercitarse los derechos de oposición, acceso, rectificación y cancelación.

La base de datos fue registrada en la agencia de protección de datos en el año 2006 y el registro actualizado en el año 2012 para dar cumplimiento a la ley vigente.

La ubicación del servidor donde se almacene la información clínica será la sede de ******EMPRESA.2., (…)****.*

El ente encargado del Tratamiento de datos y muestras será GETECCU."

Con fecha 07 de julio de 2023, desde esta Agencia se dirigió correo electrónico a GETECCU solicitando aportación de información adicional a la trasladada en la notificación inicial. En fecha 11 de julio de 2023 se recibió correo electrónico de respuesta por parte de GETECCU aportando la siguiente información relevante:

- Sobre los datos afectados, afirmaban:

  "*Se trata de Ficheros CSV con datos estructurados. Los datos personales afectados son:* ***(…)***.

  "*Por lo que respecta a la base de datos* ******PROYECTO.1****, afectada por el Ciberataque, GETECCU es el responsable del tratamiento y* ******EMPRESA.1****, como proveedor tecnológico, el encargado de tratamiento*".

  "Por todo ello en rden a la comunicación a los interesados se ha acordado lo siguiente:

  -Comunicación de la brecha a los Centros Hospitalarios.

  *Ya se ha practicado la comunicación de la brecha a todos los centros hospitalarios en los que se realiza el proyecto ***PROYECTO.1, hayan sido afectados sus (...) o no. De esta manera mantenemos reuniones con los DPD de cada Hospital informando puntualmente de la evolución de la brecha y de las medidas implementadas hasta este momento. Proseguiremos con la información y envío de la auditoria y de las medidas definitivamente implementadas.*

  -Comunicación de los (...) afectados a aquellos Centros Hospitalarios que lo soliciten.

  -Comunicación de la brecha en la web https: geteccu.org" (sic)

- Adjuntaban archivo PDF con la comunicación de la brecha que GETECCU realizó a los investigadores médicos pertenecientes a los centros hospitalarios afectados (en fechas 22 de junio de 2023 y 3 de julio de 2023). De su contenido destaca la siguiente afirmación:

  "*Le recordamos que, de conformidad con el artículo 33, apartado 1, del RGPD, su centro, como responsable/corresponsable del tratamiento de datos, debe informar a la autoridad de control competente de la violación de los datos (a más tardar 72 horas después de haber tenido conocimiento de la misma), ya que existe un riesgo potencial para los derechos y libertades de las personas físicas*".

- Adjuntaban archivo Excel que incluye un análisis del nivel de riesgo de la brecha, aportando los siguientes datos relevantes:

  - Volumen de afectados: ***(…)***

  - Tipología de datos: Sensibles.

  - Impacto: Inconvenientes importantes.

  - Riesgo Total: 32 (ALTO).

  "Como consecuencia del resultado de la calculadora de riesgo, consideramos que no es necesaria una comunicación individual al paciente, teniendo en cuenta, además, que el número de afectados y los datos de comunicación con ellos, supondría un esfuerzo desproporcionado."

- Adjuntaban archivo Excel con el listado de hospitales y volumen de personas afectadas.

CUARTO: 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).

QUINTO: En fecha 9 de agosto de 2023 se recibió notificación de brecha de datos personales por parte del ***CENTRO.55, con, entre otra, la siguiente información:

- *Introduzca una breve descripción de lo ocurrido. "Esta notificación es la continuación de la comunicación presentada por GETECCU el 19/06/2023 y que damos por reproducida. Acceso no consentido a archivos del sistema de almacenamiento secundario, con borrado y posible descarga de los mismos."*
- *Tipos de datos afectados:* ***(…)***
- *Las personas afectadas tienen los siguientes perfiles:* ***(…)***
- *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 10/07/2023*
- Se identifica el ***CENTRO.55 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha

SEXTO: En fecha 10 de agosto de 2023 se recibió notificación de brecha de datos personales por parte del ***CENTRO.1 con, entre otro, el siguiente contenido relevante:

- *Introduzca una breve descripción de lo ocurrido "Esta notificación es la continuación de la comunicación presentada por GETECCU el 19/06/2023 y que damos por reproducida. Acceso no consentido a archivos del sistema de almacenamiento secundario, con borrado y posible descarga de los mismos."*
- *Tipos de datos afectados* ***(…)***
- *Las personas afectadas tienen los siguientes perfiles:* ***(…)***
- *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 08/08/2023*
- Se identifica el ***CENTRO.1 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha

Con fecha 6 de septiembre de 2023 tuvo entrada en esta Agencia una ampliación de información de la brecha notificada previamente por el ***CENTRO.1, en el que la información inicialmente proporcionada se mantenía intacta, a excepción de (entre otra):

- *En total, ¿cuántas personas han visto sus datos 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: 06/09/2023*
- *Número de personas informadas **(…)***
- *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*

SÉPTIMO: En fecha 17 de agosto de 2023 se recibió notificación de brecha de datos personales por parte de la ***CENTRO.53 con, entre otra, la siguiente información relevante:

- *Introduzca una breve descripción de lo ocurrido. "Esta notificación es continuación de la comunicación presentada por GETECCU el 19/06/2023 y que damos por reproducida. Acceso no consentido a archivos del sistema de almacenamiento secundario, con borrado y posible descarga de los mismos."*
- *Tipos de datos afectados: **(…)***
- *Las personas afectadas tienen los siguientes perfiles: **(…)***
- *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 10/07/2023*
- *¿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: 18/08/2023*
- *Medio por el que se informará: Comunicado público o publicación en web corporativa*
- Se identifica la ***CENTRO.53 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha

OCTAVO: En fecha 25 de agosto de 2023 se recibió notificación de brecha de datos personales por parte de ***CENTRO.2 con, entre otra, la siguiente información relevante:

- *Introduzca una breve descripción de lo ocurrido. "Detección de una brecha de seguridad referida al encargado de tratamiento de datos *****EMPRESA.1,** del Proyecto *****PROYECTO.1**, del Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa GETECCU que afecta a la información provista al proyecto por parte del Hospital Universitario Río Hortega (HURH) de Valladolid."*
- *Tipos de datos afectados: De salud (otros datos de salud)*
- *Las personas afectadas tienen los siguientes perfiles: **(...)***
- *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: 14/06/2023*

- *¿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: 31/08/2023*
- *Medio por el que se informará: Comunicado público o publicación en web corporativa*
- Se identifica el ***CENTRO.2 como responsable del tratamiento y se indica que no hay implicado un encargado de tratamiento en la brecha de datos personales

NOVENO: 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.

1. En relación con los resultados de las actuaciones de investigación al ***CENTRO.54 (en adelante ***CENTRO.54):

El 5 de julio de 2023 este organismo notificó a esta Agencia la brecha de datos personales sufrida por ***EMPRESA.1** y se identificó al propio ***CENTRO.54 como responsable del tratamiento y a GETECCU como encargado.

El 8 de febrero de 2024 se recibió un escrito por parte de ***CENTRO.54, en respuesta a requerimiento de esta Agencia, en el que se adjuntan, entre otros, los siguientes documentos relevantes:

- Documento 1.4: con captura de pantalla de correo electrónico enviado desde GETECCU (dirección de correo ***EMAIL.1**) al ***CENTRO.54, el 3 de julio de 2023 con el siguiente contenido, entre otros:

  *"- Si han sido afectados datos de (...) del ***CENTRO.54, ¿de qué volumen estamos hablando?*

  ***(...)** aproximadamente*

  (…)

  Aunque el sistema de almacenamiento secundario estaba encriptado, ha podido ser desencriptado por acceso del ciberdelincuente a un token programático de seguridad. Por tanto, los datos han podido ser desencriptados."

- Documento 02: con el Registro de Actividades de Tratamiento de ***CENTRO.54 en el que figura la actividad de tratamiento de nombre "*Investigación*", que indica que trata los siguientes datos personales:

  "• Identificativos: Nombre apellidos, NIF, Contacto, domicilio teléfono, Firma, Rasgos físicos, TIS, SS

  • Datos especialmente protegidos: Salud, Vida sexual

• *Características personales:Fecha y lugar nacimiento, Estado Civil, Edad, Sexo, Nacionalidad, Datos familia (padre, madre….),Características físicas o antropométricas.*
• *Circunstancias sociales: Aficiones, estilo de vida*."

En este documento se indica como base jurídica para tal tratamiento "*El consentimiento del interesado/a para el tratamiento de sus datos personales.*"

- Documento 03: en relación con la comunicación de la brecha a los afectados se afirmaba:

"*La comunicación de la brecha a las personas afectadas la realizó GETECCU desde su web, tal y como puede comprobarse en el siguiente enlace: ***URL.1*".

Se aporta captura de pantalla con el contenido de este enlace, en el que puede verse la siguiente comunicación:

"Estimado/a paciente:

Desde la Sociedad Científica "Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU)", en nuestra condición de Responsables del Tratamiento de Datos, nos ponemos en contacto con Usted para comunicarle una incidencia
*que ha afectado a información incluida en el Estudio Nacional en Enfermedad Inflamatoria Intestinal sobre Determinantes Genéticos y Ambientales (Proyecto "***PROYECTO.1"), en el que se gestionan datos de (...) con Enfermedad Inflamatoria Intestinal con fines estadísticos y científicos. Su centro hospitalario participa en dicho proyecto.*
En este sentido, ***(…)****, constatándose que se trataba de un ciberataque intencionado y doloso. De forma inmediata se establecieron las medidas necesarias para bloquear dicho ataque y se procedió a diseñar e implementar medidas adicionales de seguridad técnicas y organizativas. Al mismo tiempo, se procedió a comunicar la brecha de seguridad a la AGENCIA ESPAÑOLA DE PROTECCION DE DATOS en cumplimiento estricto de la normativa.*
Entre la información sustraída, se encuentran ***(…).***

*Quisiéramos señalar que en el proyecto "***PROYECTO.1", se utilizan los más altos niveles de seguridad, tanto técnicos como organizativos. Los procesos de seguridad son auditados anualmente y la infraestructura tecnológica usada es reconocida mundialmente por sus elevados estándares de seguridad y robustez. No obstante, y tal como es conocido, desgraciadamente ningún sistema es totalmente inexpugnable.*
Lamentamos profundamente las molestias o inquietud que esta situación pudiera ocasionarle. Si necesita alguna aclaración no dude en comunicarse con nosotros a través del siguiente correo electrónico legal@geteccu.org dónde estaremos a su disposición para atenderle.

Atentamente,
Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU)

Nota adicional sobre medidas de seguridad recomendadas a raíz del incidente expuesto:
Le recomendamos que considere las siguientes medidas de seguridad y preventivas relacionadas con posibles mensajes que pudiera recibir:
1) A menos que su hospital utilice habitualmente el correo electrónico para contactar con usted, desconfíe de cualquier mensaje relacionado con su enfermedad, y bórrelo, ***(…).***
2) De igual forma, si recibe algún otro tipo de mensaje (telefónico, SMS, correo postal o por cualquier otra vía) que considere sospechoso por no tratarse de una forma de contacto habitual de sus médicos u hospital, ***(…)****. En cualquier caso, es importante que tenga en cuenta esas recomendaciones, ya que son medidas generales de seguridad y protección que conviene tomar siempre, independientemente de este incidente."*

- Documento 05: con el contrato de encargo de tratamiento suscrito entre ***CENTRO.54, y GETECCU, de fecha 18 de septiembre de 2023. De su análisis se extrae:

  "*El ***CENTRO.54, como responsable de tratamiento, autoriza a GETECCU a tratar por su cuenta los datos de carácter personal en la medida que ello resulta necesario para prestar el servicio indicado*".

  "*La empresa GETECCU declara estar capacitada para ofrecer las garantías suficientes, aplicando medidas técnicas y organizativas apropiadas, de manera que el tratamiento de los datos personales sea conforme con los requisitos del RGPD y de la LOPDyGDD, y se compromete a garantizar la protección de los derechos de los interesados*"

  "GETECCU ha adoptado las medidas de seguridad adecuadas para garantizar la confidencialidad, la integridad y disponibilidad de la información así como la resiliencia permanente de los sistemas de tratamiento en caso de incidencia física o técnica; implantando, conforme a la Disposición Adicional Primera de la LOPDyGDD, las medidas de seguridad que le son de aplicabilidad recogidas en el Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica para un sistema de información con la siguiente categorización de seguridad: MEDIO"

- Documento 06.2: captura de pantalla que acredita correo electrónico recibido desde GETECCU en fecha 26 de junio de 2023 con la notificación del incidente, con el siguiente contenido:

"Estimado Investigador,
*En relación al estudio titulado " Estudio Nacional en Enfermedad Inflamatoria Intestinal sobre Determinantes Genéticos y Ambientales (***PROYECTO.1)" nos ponemos en contacto con Usted para comunicarle, de manera fehaciente, que desde ***EMPRESA.1 (la empresa tecnológica que gestiona ***PROYECTO.1) se ha detectado un acceso no autorizado a un sistema 2 secundario de almacenamiento que afecta directamente a los datos personales de (...) de ***PROYECTO.1 que estaban incluidos en el mismo. En cuanto a la plataforma ***PROYECTO.1, confirmamos que no ha sido afectada en ningún momento por el ataque y opera con normalidad. El elemento atacado en cuestión, es un sistema secundario de almacenamiento que no interfiere con la operativa diaria y por tanto no afecta a la utilización de ***PROYECTO.1.*
Por favor, remita esta información al Delegado de Protección de Datos (DPO) de su centro (verifique por favor antes si su hospital está en la lista de aquellos que podemos confirmar que han sido afectados y que acompañamos al presente mail).
Continuaremos informando sobre cualquier nuevo detalle acerca de este incidente con la mayor celeridad posible
Atentamente,"

- Documento 08.1: con el análisis de riesgos de la actividad afectada, que incluye:
  - Análisis del ciclo de vida de los datos y descripción del tratamiento.
  - Análisis de 39 factores de riesgo y listado de medidas seleccionadas para mitigarlos, destacan los siguientes factores relacionados con la brecha:
    - ***(…)***

- Documentos 08.2, 08.3 y 08.4: con la relación de medidas de seguridad implantadas por ******EMPRESA.1***, anteriores a la brecha, las implantadas para reducir el riesgo de recibir un ataque similar y nuevas medidas para evitar incidentes, respectivamente. Estos documentos se analizarán más adelante, en la documentación aportada por GETECCU.

- Documento 10: en relación con el motivo por el que la brecha no fue notificada en plazo de 72 horas tras la detección, afirmaron:

  "*El 26 de junio de 2023 GETECCU informó al Investigador Principal acerca de la brecha sucedida. Se interpretó que la brecha había sido comunicada por el encargado del tratamiento, sin embargo, al ser comunicada el 30 de junio al Servicio de Administración Electrónica, Seguridad y Gestión de Procesos del ***CENTRO.54 (en ese momento Sección de Seguridad y Servicio Al Usuario), tal y como puede verse en el documento 6.2,y tras las investigaciones realizadas junto con el proveedor se consideró necesario notificarla también por parte del ***CENTRO.54, tal y como realizó".*

2. En relación con los resultados de las actuaciones de investigación a ***CENTRO.3 (en adelante, ***CENTRO.3):

El 17 de agosto de 2023 este organismo notificó a esta Agencia la brecha de datos personales sufrida por ***EMPRESA.1** y se identificó a la ***CENTRO.3 como responsable del tratamiento y a GETECCU como encargado.

El 9 de febrero de 2023 se recibió un escrito por parte de ***CENTRO.3, en respuesta a requerimiento de esta Agencia. De su análisis se extrae la información relevante:

- Afirman que el número de personas afectadas por parte de este centro es de ***(…)*** (...).

- Aportan copia de contrato suscrito entre ***CENTRO.53 y GETECCU, con fecha de firma 15 de marzo de 2018, que incluye anexo con la relación de medidas de seguridad. Se autoriza la contratación de ***EMPRESA.1** como proveedor de la plataforma tecnológica. El anexo con las medidas de seguridad es el mismo que aportó GETECCU como modelo de plantilla a incluir en los contratos formalizados con los centros, este documento incluye apartado "*Tabla 2.11 con la relación de medidas de seguridad relevantes a implementar",* que se analizará más adelante.

- Aportan documento con la comunicación de la brecha a los afectados por parte de GETECCU. El contenido es el mismo al aportado por el ***CENTRO.54, transcrito anteriormente.

- Aportan documento con la notificación de la brecha recibida desde GETECCU, con fecha 22 de junio de 2023 (y actualización posterior el 3 de julio de 2023). De este último documento se extraen las siguientes afirmaciones:

  (…)

- No acreditan análisis de riesgos ni EIPD para las actividades afectadas por la brecha, ambas solicitadas en requerimiento.

3. En relación con los resultados de las actuaciones de investigación a ***CENTRO.4 (en adelante ***CENTRO.4):

El 9 de agosto de 2023 este organismo notificó a esta Agencia la brecha de datos personales sufrida por ***EMPRESA.1** y se identificó al ***CENTRO.4** como responsable del tratamiento y a GETECCU como encargado.

El 12 de febrero de 2024 se recibió un escrito por parte de ***CENTRO.4, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido:

- *"Tras varias conversaciones con la empresa y otros Hospitales participantes en el proyecto, finalmente, se formaliza documento el 19 de junio de 2013, en el que se informa que GETECCU es quien se hace cargo del fichero y, al mismo tiempo, firmaría un contrato con ***EMPRESA.1 como encargado de tratamiento. Se adjunta como DOCUMENTO Nº 1 documento firmado el pasado 19 de junio de 2013."*

- "*Sin perjuicio de la actuación realizada por parte de ***EMPRESA.1 y GETECCU y la comunicación a la AEPD en plazo (responsable del tratamiento), los distintos Centros comunicamos la brecha por responsabilidad proactiva atendiendo a lo referido por el Delegado de Protección de Datos de la Gerencia Regional de Salud. Del mismo modo se procedió a notificar la brecha a través de un comunicado en nuestro portal WEB (al igual que el resto de Hospitales afectados de la red SACYL)"*.

- Se adjunta como Documento 1 la copia del contrato de 19 de junio de 2013. De su contenido se extrae la parte correspondiente a la responsabilidad de los datos:
  - El contrato lo suscribe ***CENTRO.55, a quien se identifica como "*Responsable inicial del fichero*", y GETECCU, a quien se identifica como "*Responsable del fichero-Encargado de tratamiento*".
  - Cláusula cuarta: "*En cumplimiento de lo establecido en el párrafo anterior, el RESPONSABLE INICIAL DEL FICHERO autoriza mediante la firma del presente contrato al RESPONSABLE DEL FICHERO -ENCARGADO DEL TRATAMIENTO:*
    1.- La subcontratación de los servicios de TRATAMIENTO DE LOS DATOS CEDIDOS a la entidad ******EMPRESA.2.*** *(…)"*
  - Anexo A: incorpora anexo con relación de medidas de seguridad, destacando las siguientes:
    "*IDENTIFICACIÓN/AUTENTICACIÓN:*
    (…).
    CONTROL DE ACCESO:
    (…)

- Se adjunta como Documento 5 comunicado público realizado por ***CENTRO.4 a través de la página web, si bien no incorpora fecha de publicación, con el siguiente contenido:

  *"COMUNICADO SOBRE UNA BRECHA DE SEGURIDAD EN EL ESTUDIO NACIONAL EN ENFERMEDAD INFLAMATORIA INTESTINAL SOBRE DETERMINANTES GENÉTICOS Y AMBIENTALES ****PROYECTO.1"*
  *Desde la Gerencia del ***CENTRO.55, en su condición de responsable del Tratamiento de Datos, se comunica una incidencia que ha afectado a información personal incluida en el Estudio Nacional en Enfermedad Inflamatoria Intestinal sobre Determinantes Genéticos y Ambientales (Proyecto "****PROYECTO.1****", en el que se gestionan datos de (...) con Enfermedad Inflamatoria Intestinal con fines estadísticos y científicos. El ***CENTRO.55 participa en dicho proyecto.*
  En este sentido, el encargado del Tratamiento de Datos del Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU), ha detectado una incidencia de seguridad, constatándose que se trataba de un ciberataque intencionado y doloso.
  De forma inmediata se establecieron las medidas necesarias para bloquear dicho ataque y se procedió a diseñar e implementar medidas adicionales de seguridad técnicas y organizativas. Al mismo tiempo, el encargado del tratamiento procedió a comunicar la brecha de seguridad a la AGENCIA ESPAÑOLA DE PROTECCION DE DATOS en cumplimiento estricto de la

normativa. Posteriormente, esta Gerencia comunicó igualmente este incidente a la Agencia Española de Protección de Datos'.
Entre la información sustraída, se encuentran datos identificativos y datos de salud de (...) de este centro hospitalario.
Hasta la fecha actual, no tenemos constancia de la materialización de un perjuicio efectivo para ninguna de las personas afectadas. Y con respecto a la información clínica, se confirma que no ha sido alterada ni eliminada, por lo que los especialistas siguen teniendo acceso a la misma con total fiabilidad.
Lamentamos profundamente las molestias o inquietud que esta situación pudiera ocasionar a los (...) afectados. si alguno necesita alguna aclaración no dude en comunicarse con nosotros a través del siguiente correo electrónico (gerente.cabu@saludcastillayleon.es), donde estaremos a su disposición para atenderle.
*Gerencia del ***CENTRO.55."*

El 12 de febrero de 2024 se recibió un escrito por parte de ***CENTRO.4, en respuesta a requerimiento de esta Agencia, en el que se adjuntaba documentación que le había aportado GETECCU.

En ninguno de estos dos escritos se acreditó la existencia de un análisis de riesgo ni EIPD para la actividad de tratamiento afectada (solicitado en requerimiento).

4. En relación con los resultados de las actuaciones de investigación al GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (en adelante, GETECCU):

El 21 de febrero de 2024 se recibió un escrito por parte de GETECCU, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido:

- Se adjunta como documento 01 un documento redactado por ******EMPRESA.1*** con una descripción de los hechos, con las causas del incidente e información sobre las medidas implantadas por esta entidad, de este documento se extraen las siguientes afirmaciones relevantes (el subrayado es nuestro):

  *"El miércoles 14 de junio de 2023, en *****EMPRESA.1** se detectó una incidencia **(…)**. (…) De forma inmediata se activaron medidas para bloquear el acceso y conocer los detalles del alcance del incidente, y se constituyó un equipo de respuesta a crisis de seguridad con personal interno y especialistas externos. (…) Desde el mismo día del ataque se llevó a cabo la implementación de nuevas medidas técnicas y organizativas adicionales, sobre las existentes capas de seguridad y políticas de la compañía, para conferir el mayor grado de seguridad posible tanto al sistema afectado, como al resto de la arquitectura y a la propia empresa".*

  *"La brecha de seguridad se originó en **(…).***

  "Se comparte listado preliminar con las principales medidas adoptadas por el proveedor tecnológico inmediatamente tras el incidente:

(…)

Además de las medidas adoptadas inmediatamente tras el incidente, se estableció un conjunto adicional de medidas técnicas y organizacionales a implementar con toda la celeridad posible. Estas medidas fueron implementadas a lo largo de las siguientes semanas:

(…)

- Se adjunta como documento 02 la plantilla que se incluye cuando se formaliza nuevo contrato entre GETECCU y un Centro Hospitalario que desea incorporarse al proyecto ******PROYECTO.1***. En este documento se incorpora la siguiente aclaración: "ESTE ANEXO DEBE SER INCLUIDO EN EL ACUERDO ENTRE GETECCU Y CADA NUEVA ORGANIZACIÓN PARTICIPANTE EN EL PROYECTO." Además, esta plantilla incluye los siguientes párrafos relevantes:

  (…)

- Se adjunta como documento 03 captura de pantalla de un correo electrónico desde la dirección ******EMAIL.2,*** dirigido a las direcciones ******EMAIL.3, ***EMAIL.4, ***EMAIL.1,*** el 16 de junio de 2023 a las 3:49 PM, con el siguiente contenido:

  "*Estimados **A.A.A., B.B.B. y C.C.C.**, tal como os ha anticipado **D.D.D.**, os remitimos a continuación el siguiente comunicado relativo al ataque que hemos sufrido. Os mantendremos puntualmente informados sobre la evolución del análisis que estamos realizando. Tanto **D.D.D.** como yo estamos a vuestra entera disposición para cualquier cuestión relacionada. Un saludo.*

  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. Concretamente, y pese a que en este momento continuamos inmersos en un proceso de investigación, trabajando diligentemente para determinar la magnitud y el alcance del ataque, mediante la presente ponemos a su disposición la información sobre la que tenemos constancia a fecha actual:*

  (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 archivos del sistema de almacenamiento secundario con borrado y posible descarga de los mismos.
  *(iii) Proyectos afectados: ***PROYECTO.1.*
  (iv) Número potencial de datos afectados: 83067

(v) Categorías de datos afectados: - Datos identificativos - Datos de contacto - Datos de salud
(vii) Medidas adoptadas para poner remedio a la violación de seguridad y mitigar riesgos por parte de ******EMPRESA.1:*** *Nuestra prioridad es proteger la privacidad de los afectados, motivo por el cual desde* ***(...)***
*Asimismo, aprovechamos la presente comunicación, en nuestra condición de Encargados del Tratamiento de los datos, y de conformidad con el artículo 33.2 del RGPD, para transmitirle nuevamente nuestra voluntad de colaborar en todo momento en aras a que Usted pueda llevar a cabo la correspondiente comunicación ante la Agencia Española de Protección de Datos****"***

- Se adjunta como documento 04.1 captura de pantalla de un correo electrónico remitido desde GETECCU (******EMAIL.1***), el 26 de junio de 2023, a los destinatarios ******EMAIL.5, ***EMAIL.6, ***EMAIL.7, ***EMAIL.8, ***EMAIL.9, ***EMAIL.10*** con el siguiente contenido:

> *"Estimado investigador, En relación al estudio titulado "* ***(***PROYECTO.1)****" nos ponemos en contacto con Usted para comunicarle, de manera fehaciente, que desde* ******EMPRESA.1*** *(la empresa tecnológica que gestiona* ******PROYECTO.1****) se ha detectado un acceso no autorizado a un sistema secundario de almacenamiento que afecta directamente a los datos personales de (...) de* ******PROYECTO.1*** *que estaban incluidos en el mismo. En cuanto a la plataforma* ******PROYECTO.1****, confirmamos que no ha sido afectada en ningún momento por el ataque y opera con normalidad. El elemento atacado en cuestión, es un sistema secundario de almacenamiento que no interfiere con la operativa diaria y por tanto no afecta a la utilización de* ******PROYECTO.1****.*
>
> *Por favor, remita esta información al DPO de su centro (verifique por favor antes si su hospital está en la lista de aquellos que podemos confirmar que han sido afectados y que acompañamos en este email)****".***

- Se adjunta como documento 04.2 y 04.3 captura de pantalla de otros dos correos electrónicos, con idéntico contenido al anterior y con fecha de envío 26 de junio de 2023, enviado desde GETECCU (******EMAIL.1***) a más de 40 direcciones de correo distintas, estas podrían corresponder a los centros hospitalarios afectados por la brecha, no obstante no se visualizan en la captura aportada, se solicita en nuevo requerimiento de información para que aclaren este aspecto.

- Se adjunta como documento 05, en respuesta a la solicitud de esta Agencia para que aporten información aclaratoria sobre los roles en protección de datos asumidos por cada entidad en el proyecto ******PROYECTO.1***, un documento de GETECCU en el que afirman:

> "*Para participar en el proyecto* ******PROYECTO.1****, los centros interesados consiguen la aprobación de su Comité Ético local y firman un contrato con GETECCU y el investigador, médico especialista del centro*

hospitalario y asociado de GETECCU. Tras ello, el centro accede a la página web donde se halla ubicada la base de datos".

"*GETECCU recibe información anonimizada (no datos personales), por lo que no llega a tratar datos personales que identifiquen, o hagan identificables, a personas físicas. (…) Por tanto, al no existir un tratamiento de datos personales por procesar información anonimizada, recayendo dicho procesamiento fuera del RGPD, no se puede entender que exista un responsable o un encargado del tratamiento*.

Sin perjuicio de lo anterior, subsidiariamente, para el caso de que se entendiera que sí existe un tratamiento de datos personales, y que por tanto, deben ser aplicables las figuras del responsable y, en su caso, del encargado del tratamiento, serían cada uno de los centros sanitarios el responsable del tratamiento de los datos personales, mientras que la figura de encargado del tratamiento recaería en GETECCU y la de subencargado del tratamiento en ******EMPRESA.1***. *Son estos centros sanitarios quienes recopilan la información para sus propias finalidades a través del médico que atiende al paciente, con la finalidad de prestarles asistencia sanitaria y, además, en segundo lugar, para llevar a cabo estudios que favorezcan el desarrollo de la medicina y el mejor conocimiento de las enfermedades y tratamientos, de forma que ello se revierta en una mejor y más eficiente asistencia sanitaria a los mismos.*

…la investigación es realizada en los propios centros sanitarios, participando como investigadores principales sus propios médicos, de forma directa, trasladando a organizaciones como GETECCU, las instrucciones de los datos a tratar, para qué finalidades, durante cuánto tiempo deben conservar dichos datos y qué medidas de seguridad técnicas y organizativas deben aplicarse, y todo ello queda reflejado y recogido en los correspondientes contratos de encargado del tratamiento en los que GETECCU actúa como encargado del tratamiento por cuenta y bajo las instrucciones de los centros sanitarios, y como subencargado de tratamiento, su proveedor técnico ******EMPRESA.1***.

Acreditamos las afirmaciones realizadas con la aportación, a modo de ejemplo, del contrato de encargado de tratamiento firmado con el Servicio de Salud de Navarra. Y el contrato firmado entre este mismo servicio y ******EMPRESA.1***"."

- Se aporta como documento 05.1 copia del contrato de encargo formalizado entre GETECCU y ***CENTRO.54, de 18 de septiembre de 2023. De su análisis se extraen los siguientes textos relevantes:

  *"Mediante las presentes cláusulas se establecen las condiciones que habilitan a GETECCU, para el tratamiento, por cuenta del ***CENTRO.54 (en adelante ***CENTRO.54), RESPONSABLE DE TRATAMIENTO, de los datos personales que se derivan de la prestación de servicio contratado.*

*GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CROHN, en adelante GETECCU, tratará en la medida en la que la ejecución lo haga imprescindible, datos personales de los que es responsable el ***CENTRO.54*."

"El tratamiento consistirá en la prestación del siguiente servicio: Llevar a cabo el proyecto ******PROYECTO.1****, que pretende fomentar estudios clínicos/genéticos a partir de un volumen importante de (...), así como ofrecer una herramienta común de trabajo a los miembros de GETECCU. Para ello, resulta necesario desarrollar una base de datos con la finalidad de obtener las variables seleccionadas sobre distintos aspectos de la enfermedad (epidemiológicos, clínicos, de seguridad de fármacos, etc.) para una explotación posterior con finalidad científica, que tendrá de duración la misma del proyecto.*
*El ***CENTRO.54, como responsable de tratamiento, autoriza a GETECCU a tratar por su cuenta los datos de carácter personal en la medida que ello resulta necesario para prestar el servicio indicado*."

En su anexo I consta: *"Datos objeto de tratamiento:*

- *Datos identificativos del paciente: - Nombre - Apellidos - Sexo - Fecha de nacimiento - Número de teléfono - Domicilio.*
- *Datos identificativos del facultativo designado: - Nombre – Apellidos*
- *Datos de salud: - Síntomas - Diagnóstico - Estado físico – Medicación".*

- Se adjunta como documento 06 el análisis de riesgos para la actividad de tratamiento afectada, entre ellas la actividad "*Desarrollo de Proyectos de Investigación Científica en Colaboración con Centros Hospitalarios y de Salud*". Del análisis se extrae la siguiente afirmación relevante:

  En su apartado relativo a "Seguridad del tratamiento", el elemento "Hay acceso no autorizado a datos personales" se le asigna un grado de probabilidad "Improbable", un impacto "Muy significativo" y un riesgo "Muy alto".

  Y concluye el documento:

  "*Tras la evaluación del riesgo realizada teniendo en cuenta la probabilidad de materialización de las amenazas detectadas y el impacto que dicha materialización tendría, se ha podido estimar que el nivel riesgo medio del tratamiento, teniendo en cuenta los datos personales tratados, el contexto y el entorno es MEDIO, para lo que se han aplicado medidas legales, técnicas y de carácter organizativo, de forma que el nivel riesgo, aun no siendo alto, haya sido mitigado.*
  Además de lo anterior, no se considera necesaria la realización de una evaluación de impacto ya que el riesgo medio detectado es de nivel MEDIO, de forma que las medidas implementadas son suficientes para mitigarlo.

Ello permite a GETECCU llevar a cabo sus actividades con garantías, sin perjuicio de la revisión periódica de dichas medidas legales, técnicas y organizativas con el fin de mantenerlas actualizadas.
GETECCU tiene todos sus tratamientos externalizados ya que su actividad se basa, precisamente, en la colaboración con terceros, por lo que verifica y comprueba las medidas que los terceros proveedores aplican sobre los datos personales".

- Se adjunta como Documento 7 el procedimiento implantado en GETECCU para la gestión de brechas de seguridad, si bien no contiene ni firma ni fecha de creación ni actualización. Su contenido incluye información sobre los canales para comunicar las incidencias y las obligaciones de notificación tanto a AEPD como afectados. Pero no incorpora información sobre tareas, roles y personas responsables de realizarlas. También se adjunta un documento de ***EMPRESA.1 con el título "Notificación y comunicación de incidentes" (original en inglés).

- Se adjunta como documento 08 relación con la tipología de datos afectada por la filtración, en el que afirman:

  "*Los tipos de datos afectados por el ataque fueron*:

  (…)

- Se adjunta como documento 09 explicación de cómo se introducían los datos personales en la plataforma por parte de los centros hospitalarios:

  "*Los datos se incorporan a la plataforma principal a través de formularios diseñados para la entrada de datos en el proyecto. Los usuarios (médicos gastroenterólogos de los hospitales participantes en el proyecto) acceden a dichos formularios a través de una página de Login".*

  Se aporta captura de pantalla de la pantalla de inicio de la plataforma (*Login inicial*) y captura de pantalla de la interfaz principal del software una vez se ha realizado Login, en esta se muestran las distintas pestañas que dan acceso a los formularios para recabar los datos. No se visualizan detalles del formulario para los datos de *Filiación del paciente.*

- Se adjunta como documento 10 afirmaciones proporcionadas por ******EMPRESA.1*** aclarando varios puntos del informe pericial. Se destaca (el subrayado es nuestro):
  - En relación con el motivo por el que se estaban utilizando los tokens programáticos, se afirma:
    (…)
  - En relación con las mejoras introducidas tras la brecha para la monitorización de logs, se afirma:

    (…)
  - En relación con las mejoras introducidas para la gestión de tokens programáticos, se afirma:

(…)

- En relación con las mejoras del sistema de cifrado de los datos, se afirma:

  (…)

- Se adjunta como documento 12 explicación sobre la posible utilización por terceros de los datos filtrados en la brecha:

  "*A fecha de 6 de febrero de 2024,* ******EMPRESA.1*** *no ha tenido conocimiento alguno de la utilización de los datos personales afectados por el ciberataque del pasado 14 de junio de 2023, por parte de ningún tercero".*

- Se adjunta 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", con el plan de acción con la relación de medidas reactivas implantadas para evitar incidentes similares. De su análisis se extraen las siguientes afirmaciones (el subrayado es nuestro):

  (…)

El 18 de abril de 2024 se recibió un segundo escrito por parte de GETECCU, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido:

- En relación con la posible dilación temporal en la notificación a los centros hospitalarios, se afirma:

  "*En primer lugar, conviene insistir en que GETECCU es una asociación científica, por lo que no se debe comparar la rapidez de los procesos de toma de decisiones y de llevar a cabo las mismas con otro tipo de entidades más habituadas al tráfico mercantil. La Junta Directiva de la Asociación está formada por médicos residentes en distintas localidades de España, y que forman parte de la Asociación con el fin de investigar las enfermedades inflamatorias intestinales.*

  En segundo lugar, ponemos de manifiesto la complejidad del proyecto debido al número de centros y (...) del mismo, era necesario repasar y asegurar el alcance del incidente.

  GETECCU tuvo que investigar quién había tenido acceso a estos datos dentro del incidente de seguridad y qué medidas de precaución debían tomarse al determinar a quién notificar sobre el incidente. A su vez, tuvo que realizar una evaluación sobre cómo podría afectar la brecha de seguridad, y, como consecuencia, quién podía tener acceso a la información comprometida. Por último, si bien es cierto que el día 16 de Junio de 2023, viernes, fue cuando el presidente de la Asociación tuvo conocimiento de los hechos, primero telefónicamente y posteriormente mediante correo electrónico remitido por el proveedor tecnológico, no es menos cierto que en ese momento se desconocían los centros

afectados y el alcance del daño, por lo que nada se podía hacer. Fue el lunes 19 cuando se fueron conociendo los nombres de los centros afectados, que no fue el definitivo.

Ya el jueves se remite la notificación a los centros hospitalarios pero algo falla y no se envían correctamente los emails, llegando a solo 6 centros. De esta cuestión se da cuenta la Junta Directiva de la Asociación y procede a remitir nuevamente el correo el 26/06/2023. Acreditamos el envío del mail con fecha 22/06/23 (Documento 7)".

- En relación con el acceso por parte de GETECCU a los datos personales afectados, se afirma: "*GETECCU tiene asignado un rol que le permite exportar la información de manera anónima de la plataforma. Los procesos de anonimización de los datos se realizan en la arquitectura tecnológica, por lo que en ningún momento GETECCU dispone acceso a datos sensibles. Los datos personales afectados corresponden a las exportaciones realizadas por los centros, ya que el rol que estos tienen asociados sí les permite ver y acceder a la información personal de su centro*".

- Se adjuntan como Documentos 1-4 capturas de pantalla con los correos electrónicos que GETECCU envió los centros afectados notificando la brecha el 26 de junio de 2023, en el que puede verse las direcciones de correo electrónico a las que fueron enviados, centros hospitalarios afectados por la brecha.

- Se adjunta como Documento 5 la siguiente lista de hospitales afectados por la brecha:

  (…)

- En el escrito de respuesta a esta Agencia, se afirma: "*Entre* ******EMPRESA.1*** *y GETECCU existe un contrato de encargo del tratamiento titulado "EXHIBIT C: USE OF TECHNOLOGY AND DATA PROCESSING", vinculado al proyecto* ******PROYECTO.1****, que se adjunta* (*Documento nº 8*)." Del análisis de este documento se aporta la siguiente información:
  - El documento está firmado por ambas partes el 13 de febrero de 2019.
  - Destaca el siguiente texto en relación con los roles asumidos por cada una de las partes en el proyecto (el término *USUARIO* hace referencia al centro que utiliza la plataforma y *PRESTADOR* refiere a ******EMPRESA.1***): "*Dentro del ámbito del presente acuerdo, USUARIO es el único responsable del tratamiento, y PRESTADOR actúa como el encargado del tratamiento*.
    GETECCU es el facilitador de EL_PROYECTO y actúa como encargado de tratamiento de los datos. Asimismo GETECCU es el único responsable del tratamiento de la base de datos ******PROYECTO.1****. PRESTADOR será el encargado del tratamiento de los datos de carácter personal, titularidad de USUARIO en calidad de responsable del tratamiento, de conformidad con lo establecido en la normativa vigente en la materia en nuestro ordenamiento jurídico".*
  - ***(…)***

- El contrato incluye una tabla descriptiva con los controles y medidas de seguridad a implantar por el prestador encargado de tratamiento (el subrayado es nuestro):

(…)

- En relación con los contratos formalizados con cada uno de los centros hospitalarios afectados, se afirma:

> "*Se aporta copia de todos los contratos de encargo del tratamiento del Proyecto* ******PROYECTO.1*** *suscritos con los diferentes centros hospitalarios para los que se vienen prestando servicios, que incluyen la autorización de éstos a contratar con subencargados del tratamiento. Tal como se ha indicado en la documentación compartida, GETECCU ofrece una herramienta de trabajo común a sus miembros (el registro* ******PROYECTO.1****), con el fin de fomentar estudios clínicos en el ámbito de la Enfermedad Inflamatoria Intestinal. Para la implementación y mantenimiento técnico del proyecto, GETECCU contrató al proveedor* ******EMPRESA.2,*** *antecesor de* ******EMPRESA.1,,*** *que se subrogó en su posición, prestando dicho servicio tecnológico desde entonces*".
>
> "*Actualmente GETECCU está llevando a cabo una continua fase de adecuación de los acuerdos, que requiere unos tiempos un poco superiores a los de una entidad mercantil ordinaria, ya que los procesos de decisión y ejecución en una Sociedad Científica, precisan de la valoración de distintos órganos de gobernanza que van cambiando periódicamente. No obstante, GETECCU tiene designada a una empresa especializada, que le está dando soporte necesario, con el objetivo de acelerar todo lo posible el procedimiento de adecuación de los acuerdos.*"

Se aporta copia de los siguientes documentos y contratos de encargo formalizados (todos incluidos en anexos "*documento nº9.pdf*" y "*documento nº10.pdf*" del escrito):

- Copia de contrato de encargo suscrito entre *****CENTRO.5** (como responsable de tratamiento) y la empresa ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 3 de octubre de 2012. Incluye anexo con medidas de seguridad técnicas y organizativas.
- Copia de contrato de encargo suscrito entre ******CENTRO.6*** (como Responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 28 de julio de 2011. El contenido es el mismo que el contrato anterior.
- Copia de contrato de encargo suscrito entre ******CENTRO.7*** (se define como *Responsable inicial del Fichero*) y GETECCU (se define como *Responsable del Fichero-Encargado de Tratamiento*), con fecha de firma 10 de noviembre de 2014, incluye obligaciones de las partes y la autorización para contratar a ******EMPRESA.2*** como subencargado de tratamiento. Incluye anexo con medidas de seguridad. Destaca el siguiente párrafo: *"HOSPITAL y GETECCU mantienen una relación de colaboración profesional con la finalidad de uso del software* ******PROYECTO.1****. Que para la realización de dichos servicios es*

necesario que GETECCU acceda y gestione ficheros de datos cuya titularidad es de HOSPITAL y que contiene datos personales"

- Copia de contrato de encargo suscrito entre ******CENTRO.8*** y GETECCU, con fecha de firma 8 de marzo de 2017. Se autoriza la subcontratación de ******EMPRESA.1***. Incluye Anexo con medidas de seguridad y el tratamiento de los datos, de este se extrae el siguiente párrafo: "*Dentro del ámbito del presente acuerdo, HOSPITAL seguirá siendo titular responsable de los ficheros de gestión hospitalaria y atención médica. GETECCU es el propietario del fichero* ******PROYECTO.1****, así como encargado de tratamiento del mismo y facilitador del proyecto* ******PROYECTO.1***".
- Copia de contrato suscrito entre ******CENTRO.9***, un médico investigador del ******CENTRO.10*** y GETECCU (definido como Promotor), firmado el 18 de noviembre de 2014. Se autoriza la subcontratación de ******EMPRESA.2,*** que asume la condición de encargado de tratamiento. Destaca el siguiente párrafo: "*Los subcontratistas, que también tienen la condición de encargados de tratamiento estarán igualmente obligados al cumplimiento de las obligaciones establecidas para promotor. Promotor responderá ante el CENTRO de cualquier incumplimiento de las entidades subcontratadas*".
- Copia de contrato de encargo entre ******CENTRO.11*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 22 de febrero de 2012. Incluye las obligaciones de las partes y anexo con medidas de seguridad.
- Copia de contrato de encargo entre ******CENTRO.12*** y GETECCU, con fecha de firma 16 de enero de 2017, con los siguientes textos relevantes:

  > "*GETECCU, propietario del fichero* ******PROYECTO.1****, al no poseer los medios técnicos necesarios, ha contratado los servicios de un proveedor tecnológico que asegura la preservación e integridad y adoptará todas las medidas de seguridad para evitar cualquier mal uso o uso fraudulento de archivos informáticos utilizados o desarrollados. Todos los términos relativos al uso de la tecnología y tratamiento de datos figuran en Anexo A*".
  >
  > "*Dentro del marco del presente acuerdo, HOSPITAL seguirá siendo titular responsable de los ficheros de gestión hospitalaria y atención médica. GETECCU es el propietario del fichero* ******PROYECTO.1****, así como el encargado de tratamiento y facilitador del proyecto* ******PROYECTO.1****.*"
  >
  > "*GETECCU ha contratado la plataforma a* ******EMPRESA.1*** *que hará todos los esfuerzos para asegurar la preservación y la integridad de los documentos y/o información y adoptará todas las medidas para evitar cualquier mal uso o uso fraudulento de archivos informáticos utilizados en el marco del acuerdo*".
- Copia de contrato de encargo entre ******CENTRO.13*** y ******EMPRESA.2***, con fecha de firma 29 de marzo de 2012.
- Copia de contrato de encargo entre el ******CENTRO.14*** (como responsable inicial del fichero) y GETECCU (responsable del fichero -

encargado de tratamiento), con fecha de firma 26 de marzo de 2015. En su contenido se autoriza la subcontratación de ******EMPRESA.2***.

- Copia de contrato de encargo entre ******CENTRO.15*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 26 abril 2013. Se autoriza la subcontratación de ******EMPRESA.2*** que asume la condición de encargado de tratamiento de los datos. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ******CENTRO.16*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 6 de mayo de 2013. Se autoriza la subcontratación de ******EMPRESA.2*** que asume condición de encargado de tratamiento. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo suscrito entre ******CENTRO.17*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 13 de enero de 2012.
- Copia de contrato de encargo entre ******CENTRO.18*** y GETECCU, con fecha de firma 28 de abril de 2017. Se autoriza la subcontratación para uso de plataforma de ******EMPRESA.1.***
- Copia de contrato de encargo entre ******CENTRO.19*** Y GETECCU, con fecha 22 de octubre de 2014. Se autoriza la subcontratación de ******EMPRESA.2.***
- Copia de contrato de encargo entre ******CENTRO.20*** y GETECCU, con fecha de firma 25 de febrero de 2014. Se autoriza la subcontratación de ******EMPRESA.2***. Incorpora anexo con medidas de seguridad.
- Copia de contrato entre ******CENTRO.21*** y GETECCU, con fecha de firma enero 2019. Se autoriza la subcontratación de ******EMPRESA.1.*** Se destacan los siguientes textos:

  > *"El Hospital consiente que el investigador, una vez obtenido el consentimiento informado del paciente, acceda a los datos de su historia clínica que sean estrictamente necesarios para el desarrollo del proyecto* ******PROYECTO.1****, manteniendo el hospital la titularidad de los ficheros de gestión hospitalaria y atención médica".*
  >
  > *"GETECCU, propietario del fichero* ******PROYECTO.1****, al no poseer los medios necesarios para alojamiento y soporte informático, ha contratado los servicios de un proveedor tecnológico que asegura la preservación e integridad de los documentos o información y adoptará todas las medidas de seguridad para evitar cualquier mal uso fraudulento de archivos informáticos utilizados o desarrollados"*.

- Copia de contrato entre ******CENTRO.22***, el INVESTIGADOR PRINCIPAL y GETECCU (PROMOTOR), firmado en fecha 24 de septiembre de 2013. No se trata de contrato de encargo de tratamiento de datos personales, aunque incorpora clausula NOVENA sobre protección de los datos personales, incluyendo el siguiente texto: *"La FUNDACIÓN dispondrá de actuaciones necesarias para que el INVESTIGADOR trate la documentación, información, resultados y datos relacionados con el estudio conforme a su carácter confidencial y secreto, procurando la circulación restringida de dicha información y*

cuidando que esta obligación sea cumplida por todas las personas que deban tener acceso a ella. En relación a las obligaciones del promotor del ensayo, cuando se guarden y procesen datos personales de investigadores y (...), se deberán tomar las medidas oportunas para protegerlos y evitar el acceso a los mismos de terceros no autorizados de acuerdo con la Ley 15/99. La FUNDACIÓN reconoce la propiedad del PROMOTOR de los datos y resultados que deriven del estudio objeto del presente contrato".

- Copia de contrato de encargo entre ******CENTRO.23*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 24 febrero de 2012. Incorpora anexo con medidas de seguridad.
- Copia de un contrato formalizado entre ******CENTRO.24*** Y GETECCU, con fecha de firma 6 de junio de 2019, con el siguiente contenido en su cláusula *OCTAVA: Protección de Datos de Carácter Personal*:

  > *"El Investigador dará a los datos de los participantes el tratamiento indicado en el Protocolo. Únicamente podrán acceder a los datos personales de los sujetos las personas indicadas en la hoja de información y en el consentimiento informado".*
  >
  > *"El Promotor garantizará que los datos personales que figuran en la documentación relacionada con el estudio han sido recogidos de acuerdo con la normativa de aplicación, trasladando la información preceptiva, informando expresamente del destino de los mismos, y recabando el consentimiento por parte de los titulares de los mismos".*
  >
  > *"El responsable del tratamiento de los datos personales (por parte del Centro) es el* ***(…)****, (por parte de la entidad Gestora)* ***(…)****, (por parte del Promotor) GETECCU*".
- Copia de contrato entre ******CENTRO.24*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 12 noviembre 2013. Incorpora autorización para subcontratar a ******EMPRESA.2.*** Incorpora anexo con medidas de seguridad.
- Copia de contrato entre ******CENTRO.25*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 10 de junio 2013. Incorpora autorización para subcontratar a ******EMPRESA.2.*** Incorpora anexo con medidas de seguridad.
- Copia de contrato entre ******CENTRO.26*** y GETECCU, con fecha de firma 22 noviembre 2015, se trata de contrato general para la realización del estudio en EII, destacando el punto *9. Protección de Datos Personales* que incorpora:

  > "*El fichero o ficheros de datos personales será proporcionado por el HOSPITAL a GETECCU, en todo momento el centro conserva el derecho exclusivo de titularidad y uso del mismo, así como de todos sus procesos de actualización. GETECCU tratará los datos personales facilitados por el HOSPITAL conforme a las instrucciones dadas por este, y con las finalidades y usos exclusivamente necesarios para el desarrollo*

de la prestación de servicios detallados en presente contrato, no pudiendo usarla para fin distinto."
"*Se autoriza la subcontratación a la entidad* ***EMPRESA.2*, *que asume la condición de encargado de tratamiento*".
Incluye anexo con medidas de seguridad.

- Copia de contrato de encargo entre ***CENTRO.27*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 5 septiembre 2012.
- Copia de contrato de encargo entre ***CENTRO.28*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 7 febrero 2012. Incorpora anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.2*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 9 agosto 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo del ***CENTRO.53*** y GETECCU, con fecha de firma 15 marzo 2018. Hace referencia a la Directiva 95/46/CE. Se incluye autorización para subcontratar a ***EMPRESA.1***.
- Copia de contrato de encargo entre ***CENTRO.29*** (como responsable de tratamiento) y GETECCU (encargado de tratamiento), con fecha de firma 13 de mayo 2013. Se autoriza la subcontratación a ***EMPRESA.2.*** Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.30*** (como responsable de tratamiento) y ***EMPRESA.2*** (encargado de tratamiento), con fecha de firma 1 junio 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato entre ***CENTRO.31*** y GETECCU, con fecha de firma 8 febrero 2021. Se autoriza la contratación de los servicios de *un proveedor tecnológico para alojamiento y soporte informático* y menciona (pero no incluye) un *Anexo A* con los términos relativo a la tecnología y al tratamiento de datos (cláusula segunda del contrato).
- Copia de contrato de encargo entre ***CENTRO.32*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha 28 de marzo de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.33*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 10 de mayo de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.34*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 9 de enero de 2014. Incluye autorización para subcontratar a ***EMPRESA.1***, así como un anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.35*** (como responsable de tratamiento) y ***EMPRESA.2*** (encargado de tratamiento), con fecha de firma 30 de octubre de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***CENTRO.36*** (como responsable de tratamiento) y ***EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 29 de febrero de 2012. Incluye anexo con medidas de seguridad.

- Copia de contrato de encargo entre ******CENTRO.37*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 9 de mayo de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo de tratamiento formalizado entre ******CENTRO.38*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 21 de octubre de 2014. Incluye autorización para la subcontratación de ******EMPRESA.2.*** De su contenido destaca el siguiente texto: "*Los investigadores disociarán adecuadamente los datos personales de los sujetos incluidos en el estudio de forma que no puedan ser identificados*".
- Copia de contrato de encargo entre ******CENTRO.39*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 10 de mayo de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ******CENTRO.40*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 10 de mayo de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ******CENTRO.41*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 10 de abril de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato suscrito por ******CENTRO.42*** (como responsable de tratamiento), la ******CENTRO.43***, el Investigador Principal y GETECCU (encargado de tratamiento), con fecha de firma 12 diciembre 2017. Incorpora Anexo con medidas de seguridad. Incluye el siguiente texto: "*GETECCU ha contratado los servicios de un proveedor tecnológico que asegura la preservación y la integridad de los documentos e información, y adoptará todas las medidas, incluidas las medidas de seguridad de hardware, para evitar cualquier mal uso o uso fraudulento de archivos informáticos utilizados o desarrollados. Todos los términos al uso de la tecnología y tratamiento de datos figuran en Anexo A que se adjunta*".
- Copia de contrato de encargo entre ******CENTRO.44*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 21 de diciembre de 2013. Incluye anexo con medidas de seguridad y autorización para subcontratar a ******EMPRESA.2***.
- Copia de contrato de encargo entre ******CENTRO.45*** (como responsable de tratamiento) y ******EMPRESA.2*** (como encargado de tratamiento), con fecha de firma 9 febrero de 2012. Incluye anexo con medidas de seguridad.
- Copia de contrato de investigación biomédica entre ******CENTRO.46*** y GETECCU, con fecha de firma enero y febrero de 2023 (según actor firmante). Incorpora "*Cláusula 8: Obligaciones de las partes, confidencialidad y protección de datos*" y con el siguiente texto relevante:

  > "*Una vez transferida la información al COORDINADOR (GETECCU), el CENTRO y El INVESTIGADOR no se responsabilizan del uso que el COORDINADOR realice con los*

datos facilitados, transfiriéndose también todas las obligaciones y responsabilidades descritas en el presente acuerdo".

"*El investigador del CENTRO se compromete a poner a disposición del COORDINADOR del ESTUDIO (GETECCU) la información debidamente disociada (seudonimizada o anonimizada), es decir, sin incluir ninguna información que permita la identificación directa de los participantes en el ESTUDIO, protegiendo su identidad y cumpliendo con los requisitos legales vigentes para dicha cesión*".

- Copia de contrato de encargo entre ******CENTRO.47*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 19 de junio de 2013. Incluye autorización para subcontratar a ******EMPRESA.2***. Incluye anexo con medidas de seguridad.
- Se aporta documento firmado por el Director Gerente del ******CENTRO.48***, en fecha 21 de febrero de 2023, con el siguiente texto:

  "*Que conoce la propuesta realizada por GETECCU, como promotor, para que sea realizado en este centro el Estudio Nacional en Enfermedad Inflamatoria Intestinal, que será llevado a cabo en el servicio Aparato Digestivo por la Investigadora Principal, que se compromete a realizarlo conforme al protocolo autorizado por el CEIM y a las disposiciones que afectan.*
  Que acepta la realización de dicho Proyecto de Investigación en este Centro.".
- Copia de contrato de encargo entre ******CENTRO.49*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 24 de septiembre de 2021. Incluye autorización para subcontratar a ******EMPRESA.1***. Incluye anexo con medidas de seguridad.
- Copia de contrato de encargo entre ***HOSPITAL UNIVERSITARIO DE BURGOS*** (como responsable de tratamiento) y GETECCU (como encargado de tratamiento), con fecha de firma 19 de junio de 2013. Incluye anexo con medidas de seguridad. Incluye autorización para subcontratar a ******EMPRESA.2.***

Teniendo en cuenta la información obtenida, se confecciona la siguiente tabla que resume el impacto de afectación de la brecha:

(…)

5. En relación con los resultados de las actuaciones de investigación al ***CENTRO.50:

El 2 de septiembre de 2024 se recibió un escrito por parte del ***CENTRO.50, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido:

- En relación con la responsabilidad del tratamiento de los datos afectados, se afirma (el subrayado es nuestro):

> [la base de datos de ******PROYECTO.1***] "*… se origina a partir de un registro cuyo propietario y responsable es GETECCU y no el ***CENTRO.50 (en adelante, ***CENTRO.50)*".
>
> "*Los investigadores que participan en el Proyecto* ******PROYECTO.1*** *pueden ser autorizados por los centros para acceder a los datos de las historias clínicas (HC) de los (...) que cumplan con los requisitos de* ******PROYECTO.1*** *y volcarlos en dicha base de datos propiedad de GETECCU*".
>
> *"Desde el punto de vista de GETECCU, tal y como se define en el artículo 2 de sus estatutos: es objeto o finalidad primordial de la Asociación estimular el estudio y la investigación de la Enfermedad Inflamatoria Intestinal y procurar la homologación de criterios clínicos-terapéuticos en el diagnóstico y tratamiento de la misma, a cuyo fin se propone:*
>
> *1. Promover el desarrollo de los medios terapéuticos idóneos con su investigación a todos los niveles, básico, experimental, clínico y epidemiológico.*
> *2. Procurar la coordinación de estos medios en tono armónico y complementario.*
> *3. Estimular la uniformidad de criterios para el tratamiento de la enfermedad inflamatoria intestinal'.*
>
> *Por tanto, considerando la definición de promotor recogida en el artículo 2 del Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, como:* '*Individuo, empresa, institución u organización responsable de iniciar, gestionar y organizar la financiación de un ensayo clínico', puede considerarse que GETECCU ostenta la condición de promotor de investigación para este Proyecto*".
>
> "*En consonancia, puesto que GETECCU actúa como promotor, siguiendo los criterios establecidos por la propia AEPD tanto en el informe jurídico N/REF: 0004/2022 como en el informe N/REF: 0038/2021, se concluye lo siguiente:*
> *El promotor es responsable del tratamiento de los datos para la finalidad clínicos con medicamentos debiendo de realización de los ensayos tomar decisiones sobre los fines y los medios en los términos de las previsiones del Reglamento (UE) 536/2014 y del Real Decreto 1090/2015 que se han expuesto"*
>
> *Previsiones que son específicamente aplicables en relación con las referencias que para esta modalidad de investigación recoge el artículo 16.3 de la LAP cuando contempla los usos de la historia clínica con fines de investigación."*

"El centro sanitario es responsable del tratamiento de datos de la historia clínica en los términos establecidos en la LAP y normativa autonómica reguladora de esta materia con las finalidades previstas en dicha normativa; salvo en lo relativo a los usos de la misma para fines de investigación sanitaria en la modalidad de ensayos clínicos que, como se ha señalado, se rigen por los términos previstos en el Real Decreto de ensayos clínicos con medicamentos. Conforme a las previsiones de esta norma, su intervención como responsable del tratamiento se circunscribe a la autorización para el acceso a la historia clínica del sujeto del ensayo por parte del personal contratado por terceros, como es el caso del monitor o la CRO. Acceso que puede articularse por medio un documento distinto de un contrato y de la figura del encargado del tratamiento, en el que se establezcan las garantías específicas para el desempeño de sus funciones.

Así pues, de la reiterada doctrina de esta AEPD se deriva que el Hospital (de forma independiente al Promotor) únicamente actúa como responsable del tratamiento de los datos de la historia clínica que puedan utilizarse en la investigación. En el presente caso, el Centro, como responsable de los referidos datos de la historia clínica, ha efectuado los análisis necesarios e instaurado las medidas de seguridad que correspondan para el correcto tratamiento de dicha información.

En ese mismo sentido el citado Código de conducta determina que: 'Así, en la medida en que el Promotor determina los criterios de los participantes cuyos datos codificados deben ser incluidos en el CRD de la investigación clínica, será considerado responsable del tratamiento de dichos datos, siendo el Centro (y/o, en su caso el Investigador Principal) el responsable del tratamiento de los datos de los participantes en la investigación clínica con la finalidad de llevar a cabo la adecuada asistencia sanitaria de aquéllos en el marco y desarrollo de la investigación".

"…queda evidenciado que en este caso GETECCU, determina los fines y los medios de tratamiento de los datos personales de los participantes en el desarrollo del Proyecto ******PROYECTO.1****, siendo responsable del tratamiento de los datos personales incluidos en dicha base de datos."*

*"En relación con la función que desempeña el ***CENTRO.50 en dicho Proyecto, y teniendo en cuenta que GETECCU es el responsable de tratamiento de* ******PROYECTO.1****, es importante señalar que el Centro únicamente se ha limitado a autorizar, respecto del investigador solicitante, el acceso a las historias clínicas de sus (...), no interviniendo en ninguna fase posterior del estudio. Esto se ha realizado con el propósito de que el investigador pueda transferir la información pertinente a la base de datos de* ******PROYECTO.1****, Proyecto en el cual el profesional participa de manera independiente al Hospital. Sin que, en ningún caso, GETECCU actúe como encargado de tratamiento del Centro, toda vez que no realiza ninguna actividad por cuenta del*

Hospital sobre los datos personales recogidos en la base de datos ******PROYECTO.1****, objeto de la brecha de la que trae causa el presente requerimiento".*

"En lo que respecta a la cesión de datos de categoría especial (HC) que se realiza a los investigadores que lo solicitan, cabe entenderse que dicha cesión se encuentra legitimada conforme a lo dispuesto en el artículo 6.1 c) del RGPD, en conexión con lo dispuesto en el artículo 9.2 i) 'el tratamiento es necesario por razones de interés público en el ámbito de la salud pública'…y el artículo 9.2.j) 'el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

"…el Hospital actúa conforme a la normativa vigente, autorizando el acceso a las historias clínicas de sus (...) exclusivamente para que el investigador pueda cumplir con los fines científicos y de investigación del Proyecto ******PROYECTO.1****".*

"…en refuerzo de esta argumentación debemos señalar que, aunque el Centro haya dado su conformidad para la realización del estudio en sus instalaciones y haya autorizado el acceso a los datos de los (...) involucrados, los investigadores que quieran acceder e incluir esa información en la base de datos de ******PROYECTO.1****, deberán obtener con carácter previo, el consentimiento informado de dichos (...) para el tratamiento de sus datos y su posible comunicación a terceros".*

- En relación con la notificación de la brecha a esta Agencia y el volumen de personas afectadas, se afirma (el subrayado es nuestro):

  "*GETECCU, tras la detección de la brecha, procede a contactar con todos los investigadores que formaban parte del Proyecto para informarles sobre el incidente. Es a través de esta vía -por parte del investigador- donde el Hospital tiene conocimiento de los hechos ocurridos y se pone en contacto con el Comité Delegado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid para realizar las acciones que, en su caso, fueran necesarias, aun no siendo responsable del tratamiento de dicha base de datos. Desde el Centro se valoró el nivel de riesgo de dicha incidencia sobre los derechos de los ciudadanos afectados, utilizando para ello la herramienta interna de la Consejería de Sanidad para la gestión de brechas de seguridad, en la cual se recogió que el número de (...) afectados ascendía a un total de* ***(…)*** *y se confirmó la no necesidad de formular comunicación a la autoridad de control. Asimismo, en función del nivel de riesgo de la incidencia, teniendo en cuenta el volumen y la tipología de datos afectados y el impacto inexistente provocado en los interesados, se estimó que no resultaba necesario informar a las personas afectadas.*".

- Se adjunta como Anexo III modelo de autorización que emite el hospital al propio investigador para el acceso a las historias clínicas de los (...) (que cumplen con el criterio de muestra del proyecto*)*. De este documento se extraen las siguientes afirmaciones (el subrayado es nuestro):

  "*Autorizar a los solicitantes el acceso a las historias clínicas de los (...) que cumplan el criterio de la muestra del proyecto….*
  No obstante y, dado que el acceso es directamente sobre los (...) y registros clínicos, registros y consecuente datos que no se encuentran en régimen de disociación, será obligado que, con carácter previo, los (...) que cumplan los criterios de la muestra expidan el oportuno consentimiento para el tratamiento de datos no disociados y su comunicación a tercero que deberá constar documentado y cuya custodia compete al equipo investigador hasta la finalización del trabajo".

- Se adjunta como Anexo VI documento con el modelo de consentimiento que se entrega a los (...), del cual se extraen los siguientes párrafos relevantes (el subrayado es nuestro):

  "*En caso de que usted nos otorgue autorización, accederemos a los datos de su historia clínica que sean estrictamente necesarios y conjuntamente con otros que usted nos facilite específicamente para este proyecto serán transferidos a una base de datos construida a tal fin. El propietario y responsable de esta base de datos es el Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU), asociación sin ánimo de lucro con CIF G07762669. La ubicación del servidor donde se almacene la información clínica será la sede de* ******EMPRESA.1***…."

  "*Podrán tener acceso a los datos clínicos de los (...) participantes, convenientemente codificados, los investigadores que presenten un proyecto de investigación que haya sido aprobado por un comité de ética, una vez éste sea aprobado también por el comité científico del proyecto* ******PROYECTO.1*** *formado por un mínimo de siete médicos pertenecientes a siete centros hospitalarios españoles*"

  "*La utilización de sus datos por parte de cualquier médico o profesional de la salud con el fin de realizar estudios clínicos o epidemiológicos se hará de forma codificada, bajo un código, que no permitirá en ningún caso el reconocimiento de su identidad.*"

- Se adjunta como Anexo I documento enviado desde el Gabinete Jurídico del Hospital a un investigador del propio centro, en agosto 2012, de su contenido destaca el texto (el subrayado es nuestro):

  "*El proyecto* ******PROYECTO.1*** *es un estudio que pretende identificar determinantes genéticos y ambientales que inciden en la enfermedad inflamatoria intestinal(...) El estudio parte de la identificación de cada sujeto muestra a través del contacto clínico (asistencial) y se apoyará en dos herramientas: Biobanco y Base de Datos, siendo esta última una herramienta fundamental donde serán volcados todos los datos*

personales y de salud de (...) muestra y de las personas de su entorno, cuando proceda. La base de datos se construirá sin disociación. Tampoco habrá disociación en el uso de la historia clínica de los sujetos muestra que consientan participar en el proyecto. (…)
El responsable de la base de datos del Proyecto no es la Gerencia de cada centro participante. (…)
La Dirección Gerencia debe limitar su ámbito de actuación a expedir autorización para participación a los profesionales del Ente Público y del propio Ente Público en el proyecto ******PROYECTO.1***. *Tal autorización, sumada a los consentimientos que individualmente facilitara cada paciente (…), es suficiente.*"

6. En relación con los resultados de las actuaciones de investigación al ***CENTRO.51:

El 3 de septiembre de 2024 se recibió un escrito por parte del ***CENTRO.51, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido:

- "*Según ha comunicado GETECCU, el número de (...) afectados pertenecientes al ***CENTRO.51 han sido* ***(…)***, *desconociendo sus nombres."*

- "*La empresa subencargada del tratamiento, ***EMPRESA.1, no informó directamente al ***CENTRO.51 de la brecha, sino únicamente al encargado del tratamiento, GETECCU, que informó de la brecha a la AEPD el 11 de julio de 2023.*

  *El 26 de julio de 2023 GETECCU informó por correo electrónico a la investigadora del ***CENTRO.51, de la existencia de la brecha de seguridad de datos personales indicándole expresamente que "no es necesario que usted realice ninguna notificación al respecto". Esta información es tomada al pie de la letra por la profesional y, como consecuencia, no se informó a los responsables del centro. Este fue el motivo por el cual no se informó de la brecha a la AEPD…"*

  Se adjunta como Anexo I correo electrónico enviado el 26 de julio de 2023 desde GETECCU con, entre otro, el siguiente contenido (el subrayado es nuestro): "*Desde GETECCU, en condición de Responsable de Tratamiento de Datos, nos ponemos en contacto con usted para comunicarle una incidencia que ha afectado a la información incluida en el Proyecto ***PROYECTO.1(…)*
  Entre la información sustraída se encuentran datos identificativos y datos de salud de (...) del mencionado proyecto. (…)
  *Los IP de ***PROYECTO.1 de todos los centros han sido informados, y desde GETECCU y desde cada centro afectado se han llevado a cabo los trámites pertinentes. Por tanto no es necesario que usted realice ninguna notificación al respecto…*"

- "*Al haber tenido conocimiento de la brecha a través del requerimiento de la AEPD, los responsables del Hospital no habían tomado ninguna medida correctiva hasta la fecha.*

No obstante, y hasta conocer el alcance y consecuencias de la brecha, con fecha 28 de agosto se ha tomado la decisión de suspender el registro de nuevos (...) en el proyecto ******PROYECTO.1***.
Además se ha abierto investigación para valorar alcance de lo ocurrido, así como proceder a exigir responsabilidades"

- Se adjunta como Anexo 2 un certificado emitido por el Director Gerente del ***CENTRO.48 con fecha 21 de febrero de 2023, en el que CERTIFICA:
"*Que conoce la propuesta realizada por Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU), como promotor, para que sea realizado en este Centro el PROYECTO DE INVESTIGACIÓN titulado: " **(***PROYECTO.1**)", que será llevado a cabo en el Servicio de APARATO DIGESTIVO por la Investigadora Principal **E.E.E.**, que se compromete a realizarlo conforme al protocolo autorizado por el CEIm y a las disposiciones que le afectan.*
Que acepta la realización de dicho Proyecto de Investigación en este Centro."

- Se adjunta como Anexo 3 el modelo de consentimiento que se proporciona a los (...). De su análisis se constata que es el mismo modelo proporcionado *por* ***CENTRO.50*,* ya analizado en punto anterior.

7. Investigación en internet:

- El 10 de septiembre de 2024 esta Agencia comprueba que de la propia página web de GETECCU (*geteccu.org*) se extrae la siguiente información:

> "*El registro* ******PROYECTO.1*** *pretende fomentar estudios clínicos/genéticos a partir de un gran número de (...) así como ofrecer una herramienta común de trabajo a los miembros de GETECCU. Los dos elementos fundamentales del proyecto son la base de datos y el biobanco. La base de datos ha sido desarrollada por consenso, presentada y discutida en varias de las reuniones del Grupo, y cuenta con el patrocinio de distintas compañías farmacéuticas.*
>
> *Se trata de una base de datos con distintos apartados que, además de contribuir al registro* ******PROYECTO.1****, puede ser utilizada de forma local, como registro de (...), aunque se desarrolló con la finalidad de obtener variables seleccionadas sobre distintos aspectos de la enfermedad (epidemiológicos, clínicos, de seguridad de fármacos, etc.) para una explotación común posterior con finalidad científica y translacional.*
>
> *El registro permite la explotación de la información para la realización de estudios epidemiológicos, clínicos y genéticos. Para tal fin el registro* ******PROYECTO.1*** *ha sido aprobado en su día por el Comité Ético de Investigación Clínica del ***CENTRO.52, y el registro fue inscrito en la Agencia de Protección de Datos, con lo que el uso de su información cumple todas las normativas legales.*

*Para participar en el proyecto *****PROYECTO.1** y poder beneficiarse tanto de la producción científica del mismo como de su utilidad a nivel local, los centros interesados deberán conseguir la aprobación de su Comité Ético local y firmar el contrato con GETECCU. Ello permitirá remitir al centro los códigos necesarios para acceder a la página web donde se halla ubicada la base de datos."*

*"El mantenimiento y explotación del registro *****PROYECTO.1** depende de los miembros del área de Investigación, el área de Gobierno de GETECCU y del coordinador *****PROYECTO.1**. El coordinador *****PROYECTO.1** es designado cada dos años por la Junta de GETECCU y es el responsable (junto a la secretaría científica) del mantenimiento y renovación del registro, así como de velar para que se cumplan las normas establecidas (expuestas en los correspondientes PNTs) para la solicitud y aprobación de proyectos, cesión de datos y muestras biológicas, y redacción de artículos derivados del registro *****PROYECTO.1***".

- El 10 de septiembre de 2024 esta Agencia comprueba que de la propia página web de GETECCU (*geteccu.org*) se extrae la siguiente información sobre los requisitos para participar en el proyecto ******PROYECTO.1*** (…):

  "*Para la utilización de *****PROYECTO.1** en un centro es necesario disponer de la autorización firmada por escrito del "RESPONSABLE DEL FICHERO" que es el gerente (o persona jurídica responsable) de cada hospital. Para ello se debe cumplimentar el documento de acuerdo para el tratamiento de datos…*".
  "*El RESPONSABLE DEL FICHERO (gerente o persona jurídica responsable) conserva el derecho exclusivo de titularidad y uso del mismo, así como de todos sus procesos de actualización y solicita la prestación del ENCARGADO DEL TRATAMIENTO (GETECCU) que garantiza que se cumplan todas las condiciones de seguridad establecidas en la mencionada Ley de Protección de Datos. La empresa subcontratada por GETECCU para gestionar la base de datos es *****EMPRESA.1 (…)**.*"

- El 10 de septiembre de 2024 esta Agencia comprueba que en la página web de la Sociedad Valenciana de Farmacia Hospitalaria se obtiene el siguiente documento utilizado en charla formativa sobre el proyecto ******PROYECTO.1*** (…):

  *"¿Quién, cuándo y cómo se puede solicitar un proyecto de investigación de ***PROYECTO.1?*
  *1. Todos los facultativos de los centros par0cipantes en ***PROYECTO.1 (con autorización del IP del centro)*
  2. Socio de GETECCU
  3. Para estudios clínicos se deben haber introducido variables clínicas de más de 100 (...), y más de 100 muestras de ADN para estudios genéticos

4. Tener aprobado el estudio que se solicite por parte del CEIC del Hospital al que se pertenezca
*5. Cumplimentar un formulario **(…)**"*

Contiene múltiples capturas de pantalla con los datos que se recaban e introducen en la plataforma por cada investigador, en concreto llama la atención el formulario para introducir los datos demográficos del paciente (página 9 del documento), que incluye los siguientes datos ("*Los campos con asterisco (*) son obligatorios*"): "*Nombre", "Primer Apellido", "Segundo apellido", "Dirección", "Código postal", "Ciudad", Teléfono fijo", "Teléfono móvil", "Número de historia", "Fecha de nacimiento (dd/mm/aaaa) (*)", "Hospital (*)", "Código del paciente (5 dígitos) (*)", "ID del paciente (*)", "Sexo (*)".*

- El 11 de septiembre de 2024 esta Agencia comprueba 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 recomienda no utilizar las claves de acceso de forma directa en la aplicación que necesita acceder a recursos de ******EMPRESA.4*** (tokens programáticos), utilizando en su lugar los ROLES como buena práctica de seguridad (**…**):

  *"Uso de roles de (...) para Aplicaciones y Servicios de *****APP.1** que requieren acceso a *****EMPRESA.4**:*
  *Para que las aplicaciones que se ejecutan en *****EMPRESA.3** u otros Servicios de *****APP.1** accedan a recursos de *****EMPRESA.4**, 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.3**. 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 (...) para administrar temporalmente las credenciales para las aplicaciones o los servicios que necesiten acceder a *****EMPRESA.4**. 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.3** 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 16 de septiembre de 2024 esta Agencia comprueba que en la revista científica ELSEVIER está publicado el siguiente artículo sobre el proyecto ******PROYECTO.1***, con título "*Registro *****PROYECTO.1** de GETECCU: diseño, monitorización y funciones*" (**…**), con, entre otro, el siguiente contenido:

  "La modificación de variables se ha efectuado siempre a criterio de un grupo de expertos, que incluye a los miembros del área de investigación y al presidente de la junta de GETECCU, así como a

aquellos miembros de GETECCU que la junta designó en cada momento "

"Para la creación de un nuevo registro de paciente es imprescindible cumplimentar el formulario de datos demográficos, sin el cual el sistema no permite introducir el resto de las variables. Los datos de filiación del paciente solo son visibles a nivel local para su uso asistencial y todos los registros son anonimizados a nivel central. Asimismo, cada investigador solo tiene acceso a los datos de su propio centro"

"Una vez el Comité Ético del centro participante ha aprobado el proyecto y su gerencia ha firmado el convenio con GETECCU de conformidad con el reglamento relativo a la protección de datos y el reglamento sobre los ensayos clínicos de medicamentos de uso humano, GETECCU otorga las contraseñas necesarias al investigador principal del centro y a los investigadores colaboradores para acceder localmente al registro."

- El 19 de septiembre de 2024 esta Agencia comprueba 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 comprueba 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* ***(…)*** puede verse el siguiente contenido, entre otro (el subrayado es nuestro):

  "Un antipatrón común es incrustar claves de acceso de (...) dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se requiera una clave de acceso de (...) 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 (...) para instancias de (...) , roles de ejecución para funciones ***(...)****, roles de (...) de* ***(...)*** *para el acceso de usuarios móviles y políticas de* ***(...)*** *para dispositivos IoT.*
  Cuando interactúe con terceros, es preferible que delegue el acceso a un rol de (...) con el acceso necesario a los recursos de su cuenta en lugar de configurar un usuario de (...) y enviar a ese tercero la clave de acceso secreta para ese usuario."

- El 24 de septiembre de 2024 esta Agencia comprueba 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 ***(…)*** 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.1 (…)****. 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*".

DÉCIMO: De acuerdo con el informe recogido de la herramienta AXESOR el 15 de diciembre de 2024, la entidad GETECCU 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, teniendo en consideración la incidencia de la brecha objeto del presente procedimiento respecto de los centros hospitalarios dentro del ámbito de competencia de la AEPD.

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 las presuntas infracciones cometidas, 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

Tratamiento de datos personales

Con fecha 19 de junio de 2023, GETECCU notificó a esta Agencia una brecha de datos personales, en la que se informaba de lo siguiente:

- *"Tipos de datos afectados:* ***(…)***
- *Las personas afectadas tienen los siguientes perfiles:* ***(...)"***

El 11 de julio de 2023 GETECCU presentó ante esta Agencia un escrito de ampliación de notificación de esta brecha, en el que se informaba de lo siguiente:

- *"Tipos de datos afectados* ***(…)"***

El 11 de julio de 2023 se recibió por parte de GETECCU un correo electrónico de respuesta a un correo anterior de esta Agencia en que se afirmaba: "*Se trata de Ficheros CSV con datos estructurados. Los datos personales afectados son:* ***(…)***.

En su Documento 05.1 que acompañaba a su escrito de 21 de febrero de 2024 de respuesta a requerimiento de esta Agencia, GETECCU aportó copia del contrato de encargo formalizado entre GETECCU y ***CENTRO.54, de 18 de septiembre de 2023, en el que en su anexo I constaba:

"Datos objeto de tratamiento:

- *Datos identificativos del paciente: - Nombre - Apellidos - Sexo - Fecha de nacimiento - Número de teléfono - Domicilio.*
- *Datos identificativos del facultativo designado: - Nombre – Apellidos*
- *Datos de salud: - Síntomas - Diagnóstico - Estado físico – Medicación".*

En su Documento 08 que acompañaba a su escrito de 21 de febrero de 2024 de respuesta a requerimiento de esta Agencia, GETECCU afirmó: "*Los tipos de datos afectados por el ataque fueron*:

(…)

El 10 de septiembre de 2024 esta Agencia comprobó que en la página web de la Sociedad Valenciana de Farmacia Hospitalaria se obtenía un documento utilizado en charla formativa sobre el proyecto ******PROYECTO.1*** (…) en el que podía observarse múltiples capturas de pantalla con los datos que se recaban e introducen en la plataforma por cada investigador. En concreto, en el formulario para introducir los datos demográficos del paciente (página 9 del documento), se incluyen los siguientes datos ("*Los campos con asterisco (*) son obligatorios*"): "*Nombre", "Primer Apellido", "Segundo apellido", "Dirección", "Código postal", "Ciudad", Teléfono fijo", "Teléfono móvil", "Número de historia", "Fecha de nacimiento (dd/mm/aaaa) (*)", "Hospital (*)", "Código del paciente (5 dígitos) (*)", "ID del paciente (*)", "Sexo (*)".*

Por tanto, 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 por GETECCU, toda vez que se realiza, entre otros tratamientos, la recogida y conservación de datos personales de personas físicas: *Nombre", "Primer Apellido", "Segundo apellido", "Dirección", "Código postal", "Ciudad", Teléfono fijo", "Teléfono móvil", "Número de historia", "Fecha de nacimiento (dd/mm/aaaa) (*)", "Hospital (*)", "Código del paciente (5 dígitos) (*)", "ID del paciente (*)", "Sexo (*)"*, así como datos clínicos relativos a la patología de los (...) participantes.

Responsable del tratamiento

El 19 de junio de 2023 GETECCU notificó a esta Agencia una brecha de datos personales en la que se identificaba a GETECCU como responsable del tratamiento y a ******EMPRESA.1*** como encargado del tratamiento implicado en la brecha.

El 4 de julio de 2023 la Autoridad Catalana de Protección de Datos (APDCAT) contactó a esta Agencia con motivo de haber recibido varias notificaciones de brecha de hospitales públicos catalanes dentro del ámbito de su competencia, que identificaban como encargado del tratamiento a GETECCU y subencargado del tratamiento a ******EMPRESA.1***

Se adjuntó un documento con el título "PROYECTO ******PROYECTO.1***, con, entre otro, el siguiente contenido:

"La información clínica de todos los (...) será recogida en una base de datos común del proyecto ******PROYECTO.1****. (…)*

Los investigadores participantes tendrán acceso integral a la información generada en centro, incluyendo los datos de identificación de los (...).

Los investigadores responsables de un estudio concreto tendrán acceso a la información de los (...) incluidos en el estudio particular contenida en la base de datos general y convenientemente anonimizada, en la que los casos serán solamente identificados mediante el código ******PROYECTO.1****."*

"El proyecto ******PROYECTO.1*** *se constituye en torno al Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU), quien nombrará al comité responsable del proyecto* ******PROYECTO.1*** *y estará compuesto por un número impar de miembros que a criterio de GETECCU se establecerá en 5 ó 7.*

El propietario, responsable de la base de dados y tratamiento de los datos es GETECCU.

GETECCU actuará como sociedad ante la que puedan ejercitarse los derechos de oposición, acceso, rectificación y cancelación.

La base de datos fue registrada en la agencia de protección de datos en el año 2006 y el registro actualizado en el año 2012 para dar cumplimiento a la ley vigente.

La ubicación del servidor donde se almacene la información clínica será la sede de ******EMPRESA.1.****.*

El ente encargado del Tratamiento de datos y muestras será GETECCU."

El 5 de julio de 2023 el ***CENTRO.54 (***CENTRO.54) notificó a esta Agencia la brecha de datos personales objeto del presente procedimiento, en la que se identificaba al ***CENTRO.54 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha.

El 11 de julio de 2023 se recibió en esta Agencia correo electrónico de respuesta por parte de GETECCU, en el que afirmaba: "*Por lo que respecta a la base de datos* ******PROYECTO.1****, afectada por el Ciberataque, GETECCU es el responsable del tratamiento y* ******EMPRESA.1****, como proveedor tecnológico, el encargado de tratamiento*". Se adjuntaba archivo PDF con la comunicación de la brecha que GETECCU realizó a los investigadores médicos pertenecientes a los centros hospitalarios afectados (en fechas 22 de junio de 2023 y 3 de julio de 2023), en el que podía verse: "*Le recordamos que, de conformidad con el artículo 33, apartado 1, del RGPD, su centro, como responsable/corresponsable del tratamiento de datos, debe informar a la autoridad de control competente de la violación de los datos (a más tardar 72 horas después de haber tenido conocimiento de la misma), ya que existe un riesgo potencial para los derechos y libertades de las personas físicas*".

El 9 de agosto de 2023 el ***CENTRO.55 notificó a esta Agencia la brecha de datos personales objeto del presente procedimiento, en la que se identificaba al ***CENTRO.55 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha.

El 10 de agosto de 2023 el ***CENTRO.54 notificó a esta Agencia una ampliación de información de la brecha notificada, pero se identificaba al ***CENTRO.54 como responsable del tratamiento y a ******EMPRESA.1*** como encargado del tratamiento implicado en la brecha.

El 10 de agosto de 2023 el ***CENTRO.1 notificó a esta Agencia la brecha de datos personales objeto del presente procedimiento, en la que se identificaba al ***CENTRO.1 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha.

El 17 de agosto de 2023 la ***CENTRO.53 notificó a esta Agencia la brecha de datos personales objeto del presente procedimiento, en la que se identificaba a la

***CENTRO.53 como responsable del tratamiento y a GETECCU como encargado del tratamiento implicado en la brecha.

El 25 de agosto de 2023 el ***CENTRO.2 notificó a esta Agencia la brecha de datos personales objeto del presente procedimiento, en la que se identificaba al ***CENTRO.2 como responsable del tratamiento y se indica que no hay implicado un encargado de tratamiento en la brecha de datos personales.

El 8 de febrero de 2024 se recibió un escrito por parte de ***CENTRO.54, en respuesta a requerimiento de esta Agencia, en el que se adjuntaba como Documento 05 el contrato de encargo de tratamiento suscrito entre ***CENTRO.54, y GETECCU, de fecha 18 de septiembre de 2023, en el que se estipulaba: "*El ***CENTRO.54, como responsable de tratamiento, autoriza a GETECCU a tratar por su cuenta los datos de carácter personal en la medida que ello resulta necesario para prestar el servicio indicado*".

El 9 de febrero de 2023 se recibió un escrito por parte de ***CENTRO.3, en respuesta a requerimiento de esta Agencia, en el que se aportaba copia del contrato suscrito entre el ***CENTRO.53 y GETECCU, con fecha de firma 15 de marzo de 2018, en el que se autorizaba la contratación de ***EMPRESA.1** como proveedor de la plataforma tecnológica.

El 12 de febrero de 2024 se recibió un escrito por parte de ***CENTRO.4, en respuesta a requerimiento de esta Agencia, con, entre otro, el siguiente contenido: *"Tras varias conversaciones con la empresa y otros Hospitales participantes en el proyecto, finalmente, se formaliza documento el 19 de junio de 2013, en el que se informa que GETECCU es quien se hace cargo del fichero y, al mismo tiempo, firmaría un contrato con ***EMPRESA.1 como encargado de tratamiento. Se adjunta como DOCUMENTO Nº 1 documento firmado el pasado 19 de junio de 2013."*

En la Cláusula cuarta del contrato se estipulaba: "*En cumplimiento de lo establecido en el párrafo anterior, el RESPONSABLE INICIAL DEL FICHERO autoriza mediante la firma del presente contrato al RESPONSABLE DEL FICHERO -ENCARGADO DEL TRATAMIENTO: 1.- La subcontratación de los servicios de TRATAMIENTO DE LOS DATOS CEDIDOS a la entidad *****EMPRESA.1.** (…)"*

Se adjuntaba como Documento 1 la copia del contrato de 19 de junio de 2013, en el que se identifica al Hospital Universitario de Burgos como "*Responsable inicial del fichero*", y a GETECCU como "*Responsable del fichero-Encargado de tratamiento*".

El 21 de febrero de 2024 se recibió un escrito por parte de GETECCU, en respuesta a requerimiento de esta Agencia, en el que se adjuntaba como documento 02 la plantilla que se incluye cuando se formaliza nuevo contrato entre GETECCU y un Centro Hospitalario que desea incorporarse al proyecto ******PROYECTO.1***. En este documento se incorpora la siguiente aclaración: "ESTE ANEXO DEBE SER INCLUIDO EN EL ACUERDO ENTRE GETECCU Y CADA NUEVA ORGANIZACIÓN PARTICIPANTE EN EL PROYECTO." Además, esta plantilla incluye los siguientes párrafos:

(…)

Como Documento 05 del escrito de GETECCU de 21 de febrero de 2024 se aportaba la siguiente información aclaratoria sobre los roles en protección de datos asumidos por cada entidad en el proyecto ******PROYECTO.1***:

> "*Para participar en el proyecto* ******PROYECTO.1****, los centros interesados consiguen la aprobación de su Comité Ético local y firman un contrato con GETECCU y el investigador, médico especialista del centro hospitalario y asociado de GETECCU. Tras ello, el centro accede a la página web donde se halla ubicada la base de datos*".
>
> "*GETECCU recibe información anonimizada (no datos personales), por lo que no llega a tratar datos personales que identifiquen, o hagan identificables, a personas físicas. (…) Por tanto, al no existir un tratamiento de datos personales por procesar información anonimizada, recayendo dicho procesamiento fuera del RGPD, no se puede entender que exista un responsable o un encargado del tratamiento*.
>
> *Sin perjuicio de lo anterior, subsidiariamente, para el caso de que se entendiera que sí existe un tratamiento de datos personales, y que por tanto, deben ser aplicables las figuras del responsable y, en su caso, del encargado del tratamiento, serían cada uno de los centros sanitarios el responsable del tratamiento de los datos personales, mientras que la figura de encargado del tratamiento recaería en GETECCU y la de subencargado del tratamiento en* ******EMPRESA.1***. *Son estos centros sanitarios quienes recopilan la información para sus propias finalidades a través del médico que atiende al paciente, con la finalidad de prestarles asistencia sanitaria y, además, en segundo lugar, para llevar a cabo estudios que favorezcan el desarrollo de la medicina y el mejor conocimiento de las enfermedades y tratamientos, de forma que ello se revierta en una mejor y más eficiente asistencia sanitaria a los mismos.*
>
> *…la investigación es realizada en los propios centros sanitarios, participando como investigadores principales sus propios médicos, de forma directa, trasladando a organizaciones como GETECCU, las instrucciones de los datos a tratar, para qué finalidades, durante cuánto tiempo deben conservar dichos datos y qué medidas de seguridad técnicas y organizativas deben aplicarse, y todo ello queda reflejado y recogido en los correspondientes contratos de encargado del tratamiento en los que GETECCU actúa como encargado del tratamiento por cuenta y bajo las instrucciones de los centros sanitarios, y como subencargado de tratamiento, su proveedor técnico* ******EMPRESA.1***.
>
> *Acreditamos las afirmaciones realizadas con la aportación, a modo de ejemplo, del contrato de encargado de tratamiento firmado con el Servicio de Salud de Navarra. Y el contrato firmado entre este mismo servicio y* ******EMPRESA.1***"."

Como Documento 05.1 del escrito de GETECCU de 21 de febrero de 2024 se aportaba copia del contrato de encargo formalizado entre GETECCU y ***CENTRO.54, de 18 de septiembre de 2023, en el que se estipulaba:

> *"Mediante las presentes cláusulas se establecen las condiciones que habilitan a GETECCU, para el tratamiento, por cuenta del ***CENTRO.54 (en adelante ***CENTRO.54), RESPONSABLE DE TRATAMIENTO, de los datos personales que se derivan de la prestación de servicio contratado.*
> *GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CROHN, en adelante GETECCU, tratará en la medida en la que la ejecución lo haga imprescindible, datos personales de los que es responsable el ***CENTRO.54*."
>
> *"El tratamiento consistirá en la prestación del siguiente servicio: Llevar a cabo el proyecto* ******PROYECTO.1****, que pretende fomentar estudios clínicos/genéticos a partir de un volumen importante de (...), así como ofrecer una herramienta común de trabajo a los miembros de GETECCU. Para ello, resulta necesario desarrollar una base de datos con la finalidad de obtener las variables seleccionadas sobre distintos aspectos de la enfermedad (epidemiológicos, clínicos, de seguridad de fármacos, etc.) para una explotación posterior con finalidad científica, que tendrá de duración la misma del proyecto.*
> *El ***CENTRO.54, como responsable de tratamiento, autoriza a GETECCU a tratar por su cuenta los datos de carácter personal en la medida que ello resulta necesario para prestar el servicio indicado*."

El 18 de abril de 2024 se recibió un segundo escrito por parte de GETECCU, en respuesta a requerimiento de esta Agencia, en el que se afirmaba: "*Entre* ******EMPRESA.1*** *y GETECCU existe un contrato de encargo del tratamiento titulado "EXHIBIT C: USE OF TECHNOLOGY AND DATA PROCESSING", vinculado al proyecto* ******PROYECTO.1****, que se adjunta* (*Documento nº 8*)", firmado por ambas partes el 13 de febrero de 2019. En este Documento nº 8 el término *USUARIO* hace referencia al centro que utiliza la plataforma y *PRESTADOR* refiere a ******EMPRESA.1***:

"*Dentro del ámbito del presente acuerdo, USUARIO es el único responsable del tratamiento, y PRESTADOR actúa como el encargado del tratamiento*.
GETECCU es el facilitador de EL_PROYECTO y actúa como encargado de tratamiento de los datos. Asimismo GETECCU es el único responsable del tratamiento de la base de datos ******PROYECTO.1****. PRESTADOR será el encargado del tratamiento de los datos de carácter personal, titularidad de USUARIO en calidad de responsable del tratamiento, de conformidad con lo establecido en la normativa vigente en la materia en nuestro ordenamiento jurídico".*
En el escrito de GETECCU de 18 de abril de 2024, de respuesta a requerimiento de esta Agencia, se aportaba como Documento nº 9 y Documento nº 10 copia de los documentos y contratos de encargo formalizados por GETECCU con 47 centros hospitalarios, de los que se extrae la siguiente información:

(…)

El 2 de septiembre de 2024 se recibió un escrito del ***CENTRO.50, en respuesta a requerimiento de esta Agencia, en el que afirmaba que:

[la base de datos de ***PROYECTO.1] "*… se origina a partir de un registro cuyo propietario y responsable es GETECCU y no el ***CENTRO.50 (en adelante, ***CENTRO.50)*".

"Desde el punto de vista de GETECCU, tal y como se define en el artículo 2 de sus estatutos: es objeto o finalidad primordial de la Asociación estimular el estudio y la investigación de la Enfermedad Inflamatoria Intestinal y procurar la homologación de criterios clínicos-terapéuticos en el diagnóstico y tratamiento de la misma, a cuyo fin se propone:

> *1. Promover el desarrollo de los medios terapéuticos idóneos con su investigación a todos los niveles, básico, experimental, clínico y epidemiológico.*
> *2. Procurar la coordinación de estos medios en tono armónico y complementario.*
> *3. Estimular la uniformidad de criterios para el tratamiento de la enfermedad inflamatoria intestinal'.*

Por tanto, considerando la definición de promotor recogida en el artículo 2 del Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, como: 'Individuo, empresa, institución u organización responsable de iniciar, gestionar y organizar la financiación de un ensayo clínico', puede considerarse que GETECCU ostenta la condición de promotor de investigación para este Proyecto".

"*En consonancia, puesto que GETECCU actúa como promotor, siguiendo los criterios establecidos por la propia AEPD tanto en el informe jurídico N/REF: 0004/2022 como en el informe N/REF: 0038/2021, se concluye lo siguiente:*
El promotor es responsable del tratamiento de los datos para la finalidad clínicos con medicamentos debiendo de realización de los ensayos tomar decisiones sobre los fines y los medios en los términos de las previsiones del Reglamento (UE) 536/2014 y del Real Decreto 1090/2015 que se han expuesto"

Previsiones que son específicamente aplicables en relación con las referencias que para esta modalidad de investigación recoge el artículo 16.3 de la LAP cuando contempla los usos de la historia clínica con fines de investigación."

"El centro sanitario es responsable del tratamiento de datos de la historia clínica en los términos establecidos en la LAP y normativa autonómica reguladora de esta materia con las finalidades previstas en dicha normativa; salvo en lo relativo a los usos de la misma para fines de investigación sanitaria en la modalidad de ensayos clínicos que, como se ha señalado, se rigen por los términos previstos en el Real Decreto de ensayos clínicos con medicamentos. Conforme a las previsiones de esta norma, su intervención como responsable del tratamiento se circunscribe a la autorización para el acceso a la historia clínica del sujeto del ensayo por parte del personal contratado por terceros, como es el caso del monitor o la CRO. Acceso que puede articularse por medio un documento distinto de un contrato y de la figura del encargado del

tratamiento, en el que se establezcan las garantías específicas para el desempeño de sus funciones.

Así pues, de la reiterada doctrina de esta AEPD se deriva que el Hospital (de forma independiente al Promotor) únicamente actúa como responsable del tratamiento de los datos de la historia clínica que puedan utilizarse en la investigación. En el presente caso, el Centro, como responsable de los referidos datos de la historia clínica, ha efectuado los análisis necesarios e instaurado las medidas de seguridad que correspondan para el correcto tratamiento de dicha información.

En ese mismo sentido el citado Código de conducta determina que: 'Así, en la medida en que el Promotor determina los criterios de los participantes cuyos datos codificados deben ser incluidos en el CRD de la investigación clínica, será considerado responsable del tratamiento de dichos datos, siendo el Centro (y/o, en su caso el Investigador Principal) el responsable del tratamiento de los datos de los participantes en la investigación clínica con la finalidad de llevar a cabo la adecuada asistencia sanitaria de aquéllos en el marco y desarrollo de la investigación".

"…queda evidenciado que en este caso GETECCU, determina los fines y los medios de tratamiento de los datos personales de los participantes en el desarrollo del Proyecto ******PROYECTO.1****, siendo responsable del tratamiento de los datos personales incluidos en dicha base de datos."*

*"En relación con la función que desempeña el ***CENTRO.50 en dicho Proyecto, y teniendo en cuenta que GETECCU es el responsable de tratamiento de* ******PROYECTO.1****, es importante señalar que el Centro únicamente se ha limitado a autorizar, respecto del investigador solicitante, el acceso a las historias clínicas de sus (...), no interviniendo en ninguna fase posterior del estudio. Esto se ha realizado con el propósito de que el investigador pueda transferir la información pertinente a la base de datos de* ******PROYECTO.1****, Proyecto en el cual el profesional participa de manera independiente al Hospital. Sin que, en ningún caso, GETECCU actúe como encargado de tratamiento del Centro, toda vez que no realiza ninguna actividad por cuenta del Hospital sobre los datos personales recogidos en la base de datos* ******PROYECTO.1****, objeto de la brecha de la que trae causa el presente requerimiento".*

"En lo que respecta a la cesión de datos de categoría especial (HC) que se realiza a los investigadores que lo solicitan, cabe entenderse que dicha cesión se encuentra legitimada conforme a lo dispuesto en el artículo 6.1 c) del RGPD, en conexión con lo dispuesto en el artículo 9.2 i) 'el tratamiento es necesario por razones de interés público en el ámbito de la salud pública'…y el artículo 9.2.j) 'el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

"…el Hospital actúa conforme a la normativa vigente, autorizando el acceso a las historias clínicas de sus (...) exclusivamente para que el investigador pueda cumplir con los fines científicos y de investigación del Proyecto ******PROYECTO.1****".*

"…en refuerzo de esta argumentación debemos señalar que, aunque el Centro haya dado su conformidad para la realización del estudio en sus instalaciones y haya autorizado el acceso a los datos de los (...) involucrados, los investigadores que quieran acceder e incluir esa información en la base de datos de ******PROYECTO.1****, deberán obtener con carácter previo, el consentimiento informado de dichos (...) para el tratamiento de sus datos y su posible comunicación a terceros".*

Se adjunta como Anexo I documento enviado desde el Gabinete Jurídico del Hospital a un investigador del propio centro, en agosto 2012, de su contenido destaca el texto (el subrayado es nuestro):

> "*El proyecto* ******PROYECTO.1*** *es un estudio que pretende identificar determinantes genéticos y ambientales que inciden en la enfermedad inflamatoria intestinal(...) El estudio parte de la identificación de cada sujeto muestra a través del contacto clínico (asistencial) y se apoyará en dos herramientas: Biobanco y Base de Datos, siendo esta última una herramienta fundamental donde serán volcados todos los datos personales y de salud de (...) muestra y de las personas de su entorno, cuando proceda. La base de datos se construirá sin disociación. Tampoco habrá disociación en el uso de la historia clínica de los sujetos muestra que consientan participar en el proyecto*. (…)
> *El responsable de la base de datos del Proyecto no es la Gerencia de cada centro participante. (…)*
> *La Dirección Gerencia debe limitar su ámbito de actuación a expedir autorización para participación a los profesionales del Ente Público y del propio Ente Público en el proyecto* ******PROYECTO.1****. Tal autorización, sumada a los consentimientos que individualmente facilitara cada paciente (…), es suficiente.*"

El 10 de septiembre de 2024 esta Agencia comprobó que en la propia página web de GETECCU (*geteccu.org*) constaba la siguiente información:

> "*El registro* ******PROYECTO.1*** *pretende fomentar estudios clínicos/genéticos a partir de un gran número de (...) así como ofrecer una herramienta común de trabajo a los miembros de GETECCU. (…)*
>
> *Se trata de una base de datos con distintos apartados que, además de contribuir al registro* ******PROYECTO.1****, puede ser utilizada de forma local, como registro de (...), aunque se desarrolló con la finalidad de obtener variables seleccionadas sobre distintos aspectos de la enfermedad (epidemiológicos, clínicos, de seguridad de fármacos, etc.) para una explotación común posterior con finalidad científica y translacional.*
>
> *El registro permite la explotación de la información para la realización de estudios epidemiológicos, clínicos y genéticos. (…)*
>
> *Para participar en el proyecto* ******PROYECTO.1*** *y poder beneficiarse tanto de la producción científica del mismo como de su utilidad a nivel local, los centros interesados deberán conseguir la aprobación de su*

Comité Ético local y firmar el contrato con GETECCU. Ello permitirá remitir al centro los códigos necesarios para acceder a la página web donde se halla ubicada la base de datos."

"El mantenimiento y explotación del registro ******PROYECTO.1*** *depende de los miembros del área de Investigación, el área de Gobierno de GETECCU y del coordinador* ******PROYECTO.1****. El coordinador* ******PROYECTO.1*** *es designado cada dos años por la Junta de GETECCU y es el responsable (junto a la secretaría científica) del mantenimiento y renovación del registro, así como de velar para que se cumplan las normas establecidas (expuestas en los correspondientes PNTs) para la solicitud y aprobación de proyectos, cesión de datos y muestras biológicas, y redacción de artículos derivados del registro* ******PROYECTO.1***".

El 10 de septiembre de 2024 esta Agencia comprobó que en la propia página web de GETECCU se publicó lo siguiente (…):

"*Para la utilización de* ******PROYECTO.1*** *en un centro es necesario disponer de la autorización firmada por escrito del "RESPONSABLE DEL FICHERO" que es el gerente (o persona jurídica responsable) de cada hospital. Para ello se debe cumplimentar el documento de acuerdo para el tratamiento de datos…*".
"*El RESPONSABLE DEL FICHERO (gerente o persona jurídica responsable) conserva el derecho exclusivo de titularidad y uso del mismo, así como de todos sus procesos de actualización y solicita la prestación del ENCARGADO DEL TRATAMIENTO (GETECCU) que garantiza que se cumplan todas las condiciones de seguridad establecidas en la mencionada Ley de Protección de Datos. La empresa subcontratada por GETECCU para gestionar la base de datos es* ******EMPRESA.1 (…)***."

De todo lo expuesto, se extrae que en el contrato firmado entre GETECCU y ******EMPRESA.1***, GETECCU se identifica como responsable del tratamiento respecto de los datos del Proyecto ******PROYECTO.1*** y a ******EMPRESA.1*** como encargado del tratamiento. Esta misma relación es la que consta en las notificaciones de la brecha de datos personales ante esta Agencia, realizadas por GETECCU.

No obstante, en las notificaciones de la brecha de datos personales notificadas por los distintos centros hospitalarios, son éstos los que se identifican como responsables del tratamiento, mientras que se identifica como encargado a GETECCU, excepto en la segunda notificación realizada por el ***CENTRO.54, que identifica como encargado a ******EMPRESA.1***, y en el caso del ***CENTRO.2, en la que se indica que no hay implicado un encargado de tratamiento en la brecha de datos personales.

Por su parte, respecto de los centros hospitalarios participantes en el Proyecto ******PROYECTO.1***:

- Existen contratos firmados entre los centros hospitalarios como responsables del tratamiento y la empresa ******EMPRESA.2*** (como encargado de tratamiento.
- Existen contratos de encargo entre los centros hospitalarios como "*Responsable inicial del Fichero*) y GETECCU como "*Responsable del Fichero-*

Encargado de Tratamiento"), en los que se autoriza a contratar a ******EMPRESA.2*** como subencargado de tratamiento.

- Existe contrato firmado entre el centro hospitalario y GETECCU, en el que no se especifican los roles pero se autoriza la subcontratación de ******EMPRESA.1*** y se estipula: "*Dentro del ámbito del presente acuerdo, HOSPITAL seguirá siendo titular responsable de los ficheros de gestión hospitalaria y atención médica. GETECCU es el propietario del fichero* ******PROYECTO.1****, así como encargado de tratamiento del mismo y facilitador del proyecto* ******PROYECTO.1***".
- Existe contrato firmado entre el centro hospitalario, un médico investigador y GETECCU (definido como Promotor), en el que se autoriza la subcontratación de ******EMPRESA.2,*** que asume la condición de encargado de tratamiento y estipula: "*Los subcontratistas, que también tienen la condición de encargados de tratamiento estarán igualmente obligados al cumplimiento de las obligaciones establecidas para promotor. Promotor responderá ante el CENTRO de cualquier incumplimiento de las entidades subcontratadas*".
- Existe contrato entre el centro hospitalario y GETECCU, en el que se estipula:

  "*GETECCU, propietario del fichero* ******PROYECTO.1****, al no poseer los medios técnicos necesarios, ha contratado los servicios de un proveedor tecnológico que asegura la preservación e integridad y adoptará todas las medidas de seguridad para evitar cualquier mal uso o uso fraudulento de archivos informáticos utilizados o desarrollados. Todos los términos relativos al uso de la tecnología y tratamiento de datos figuran en Anexo A*".

  "*Dentro del marco del presente acuerdo, HOSPITAL seguirá siendo titular responsable de los ficheros de gestión hospitalaria y atención médica. GETECCU es el propietario del fichero* ******PROYECTO.1****, así como el encargado de tratamiento y facilitador del proyecto* ******PROYECTO.1***."

  "*GETECCU ha contratado la plataforma a* ******EMPRESA.1*** *que hará todos los esfuerzos para asegurar la preservación y la integridad de los documentos y/o información y adoptará todas las medidas para evitar cualquier mal uso o uso fraudulento de archivos informáticos utilizados en el marco del acuerdo*".
- Existen contratos firmados entre los centros hospitalarios, un médico investigador y GETECCU (definido como Promotor), en el que se autoriza la subcontratación de ******EMPRESA.2,*** que asume la condición de encargado de tratamiento.
- Existen contratos de encargo entre los centros hospitalarios como responsables del tratamiento y GETECCU como encargado, en los que se autoriza la subcontratación de ******EMPRESA.2***, que asume la condición de encargado de tratamiento de los datos.
- Existe contrato de encargo entre el centro hospitalario como responsable del tratamiento y GETECCU como encargado, en el que se autoriza la subcontratación para uso de plataforma de ******EMPRESA.1.***
- Existe contrato firmado entre el centro hospitalario y GETECCU en el que se estipula: "*OCTAVA: Protección de Datos de Carácter Personal*:
  "El Investigador dará a los datos de los participantes el tratamiento indicado en el Protocolo. Únicamente podrán acceder a los datos personales de los sujetos las personas indicadas en la hoja de información y en el consentimiento informado".

"El Promotor garantizará que los datos personales que figuran en la documentación relacionada con el estudio han sido recogidos de acuerdo con la normativa de aplicación, trasladando la información preceptiva, informando expresamente del destino de los mismos, y recabando el consentimiento por parte de los titulares de los mismos".
"El responsable del tratamiento de los datos personales (por parte del Centro) es el ***(…)****, (por parte de la entidad Gestora)* ***(…)****, (por parte del Promotor) GETECCU*".

- Existe contrato firmado entre el centro hospitalario y GETECCU en el que se estipula: "*El fichero o ficheros de datos personales será proporcionado por el HOSPITAL a GETECCU, en todo momento el centro conserva el derecho exclusivo de titularidad y uso del mismo, así como de todos sus procesos de actualización. GETECCU tratará los datos personales facilitados por el HOSPITAL conforme a las instrucciones dadas por este, y con las finalidades y usos exclusivamente necesarios para el desarrollo de la prestación de servicios detallados en presente contrato, no pudiendo usarla para fin distinto*." Y se autoriza la subcontratación a *****EMPRESA.2**, quien actúa como encargado de tratamiento.
- Existe contrato firmado entre el centro hospitalario y GETECCU, en el que no se especifican los roles, pero se autoriza la contratación de "los servicios de *un proveedor tecnológico para alojamiento y soporte informático"*.
- Existe documento en el que el centro hospitalario acepta la realización del Proyecto, pero no se especifican los roles.

Como puede observarse, en toda la información obrante en el presente procedimiento existen discrepancias en cuanto a los roles de centros hospitalarios, GETECCU y ******EMPRESA.2 / ***EMPRESA.1*** respecto al tratamiento de los datos personales objeto del Proyecto ******PROYECTO.1***.

De acuerdo con las Directrices 07/2020 del CEPD sobre los conceptos de «Responsable del Tratamiento» y «Encargado del Tratamiento» en el RGPD, los conceptos de responsable del tratamiento y encargado del tratamiento son conceptos funcionales, siendo necesario establecerlos en virtud de sus actividades concretas en el caso analizado y no en función de la designación formal que pueda figurar en el contrato: *"12. Los conceptos de «responsable del tratamiento» y «encargado del tratamiento» son conceptos funcionales: su objetivo es asignar responsabilidades en función del papel real de cada parte. Esto implica que la condición jurídica de «responsable del tratamiento» o «encargado del tratamiento» de los participantes debe establecerse en principio en virtud de sus actividades concretas en una situación determinada y no en función de la designación formal de un participante como «responsable del tratamiento» o «encargado del tratamiento» (p. ej., en un contrato).Esto implica que la asignación de la función de responsable o encargado debe derivar normalmente de un análisis de los hechos o circunstancias del caso y, en consecuencia, no es negociable."*

Asimismo, las referidas Directrices del CEPD 07/2020 abogan por una interpretación amplia del concepto de responsable del tratamiento con el fin de promover una protección eficaz y completa de los interesados. En este sentido, prevén: *"14. Puesto que el objetivo último de la atribución de la función de responsable del tratamiento es garantizar la responsabilidad proactiva y una protección eficaz e integral de los datos*

personales, el concepto de «responsable» debería interpretarse de un modo suficientemente amplio, de manera que promueva, en la medida de lo posible, una protección eficaz y completa de los interesados , con el fin de garantizar la plena eficacia del Derecho de la Unión en materia de protección de datos, evitar lagunas y prevenir las posibles elusiones de la normativa, sin que todo ello suponga una merma de las atribuciones del encargado del tratamiento."

A lo ya expuesto, cabe añadir que dichas Directrices del CEPD destacan: *"20. (…) El responsable del tratamiento es quien decide determinados aspectos esenciales del tratamiento de los datos. La responsabilidad del tratamiento puede establecerse en la normativa o deducirse de un análisis de los hechos o las circunstancias del caso. Es necesario dirigir la atención a las actividades de tratamiento concretas de que se trate y comprender quién las determina. Para ello, primero deben examinarse las siguientes cuestiones: «¿por qué tiene lugar el tratamiento?» y «¿quién ha decidido que debe llevarse a cabo el tratamiento para un fin concreto?»."*

En relación con esta cuestión, las Directrices del CEPD 07/2020 han resaltado que los términos de un contrato no son determinantes a la hora de establecer qué parte actúa como responsable del tratamiento, siendo necesario analizar las circunstancias del caso concreto: **"***28. En muchas ocasiones, el examen de las cláusulas contractuales entre las distintas partes involucradas puede ayudar a determinar qué parte o partes actúan como responsables del tratamiento. Aun cuando el contrato no estipule quién es el responsable del tratamiento, puede contener elementos suficientes para inferir quién tiene el poder de decisión en relación con los fines y medios del tratamiento. También es posible que el contrato contenga una declaración expresa sobre la identidad del responsable del tratamiento. Si no existen motivos para dudar de que esta se ajuste a la realidad, nada se opone a que se sigan las condiciones fijadas en el contrato. No obstante, los términos de un contrato no son determinantes en todos los casos, ya que, de ser así, las partes simplemente podrían atribuir la responsabilidad como lo consideraran oportuno. No es posible devenir responsable del tratamiento ni rehuir las obligaciones del responsable mediante una mera fórmula en el contrato cuando las circunstancias de hecho indiquen lo contrario."*

El apartado 7 del artículo 4 "*Definiciones*" del RGPD indica que es responsable del tratamiento "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*…"

Las Directrices del CEPD 07/2020 indican dos condiciones fundamentales para ser considerado encargado del tratamiento:

> *"76. Para ser considerado encargado del tratamiento, es necesario reunir dos condiciones fundamentales:*
> *a) ser un ente independiente del responsable del tratamiento; y*
> *b) tratar datos personales por cuenta del responsable."*

Al respecto, esta Agencia considera que, si bien el incidente origen del presente procedimiento tuvo lugar en los sistemas de ******EMPRESA.1*** , GETECCU actúa en el presente caso como responsable del tratamiento de los datos personales afectados por la brecha en cuestión (datos del Proyecto ******PROYECTO.1***, toda vez que:

- GETECCU notificó la brecha a esta Agencia

- GETECCU informó de la brecha a través de su página web
- GETECCU informó de la brecha a los hospitales afectados
- En la plataforma principal a través de la cual se incorporan los datos por los usuarios (médicos de los hospitales participantes), para realizar el Log in se muestra logo del proyecto y membrete de GETECCU, así como en el formulario a cumplimentar. Por tanto, GETECCU es quien identifica los datos a proporcionar por los participantes en el proyecto.
- Se firmó un contrato de encargo de tratamiento, en el que GETECCU se identifica como responsable del tratamiento y ******EMPRESA.1*** como encargado.
- Existe un documento Anexo que se incluye en los acuerdos que se firmen entre GETECCU y los centros hospitalarios que participen en el Proyecto ******PROYECTO.1***, por tanto se estarían determinando las cláusulas tecnológicas y de tratamiento de datos personales que se aplicarían a las entidades participantes. Asimismo, de este documento, puede extraerse las siguientes conclusiones:
    - apartado 2.12. Datos de carácter personal:
        - *"GETECCU es el único responsable del tratamiento de la base de datos ***PROYECTO.1". Si bien los centros hospitalarios son responsables del tratamiento de los datos que incorporan al Proyecto, GETECCU lo es de todos los datos que se incorporen a la base de datos del Proyecto en cuestión, que es la que se vio afectada por la brecha objeto del presente procedimiento.*
    - "*GETECCU ha contratado la plataforma **(…)** a PRESTADOR"*. Es decir, GETECCU es quien decide sobre los fines (las características del proyecto son fijadas por GETECCU y son los centros hospitalarios los que se adhieren; es decir, éstos no pueden establecer particularidades en cuanto a los datos u objetivos del estudio, sino que se adhieren a lo ya determinado por GETECCU) y medios del tratamiento.

Por último, esta Agencia desea traer a colación los argumentos esgrimidos por el ***CENTRO.50 en su escrito de 2 de septiembre de 2024, por los que considera que GETECCU actúa como responsable del tratamiento respecto de los datos personales del Proyecto ******PROYECTO.1***, en especial en lo relativo a los criterios establecidos por la AEPD en sus informes jurídicos N/REF: 0004/2022 y N/REF: 0038/2021, al entender que GETECCU se considera promotor de la investigación del Proyecto ******PROYECTO.1***, por lo que aunque no accediera a los datos personales que se incluyen en la base de datos, no deja de ser el responsable del tratamiento de tales datos.

En efecto, GETECCU tiene por objeto estimular el estudio y la investigación de la Enfermedad Inflamatoria Intestinal y procurar la homologación de criterios clínicos-terapéuticos en el diagnóstico y tratamiento de la misma. En el presente caso, GETECCU ha impulsado y coordinado la realización del Proyecto ******PROYECTO.1***.

El artículo 2 del Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos define al promotor como: '*Individuo, empresa, institución u organización responsable de iniciar, gestionar y organizar la financiación de un ensayo clínico*', por lo que esta Agencia entiende que en el presente caso GETECCU ostenta la condición de promotor de investigación para el Proyecto

***PROYECTO.1, cuyos datos personales se vieron afectados por la brecha objeto del presente procedimiento.

En los informes jurídicos N/REF: 0004/2022 y N/REF: 0038/2021 esta Agencia ha entendido que el promotor es responsable del tratamiento de los datos para la finalidad clínicos con medicamentos debiendo de realización de los ensayos tomar decisiones sobre los fines y los medios en los términos de las previsiones del Reglamento (UE) 536/2014 y del Real Decreto 1090/2015.

Y que el centro sanitario es responsable del tratamiento de datos de la historia clínica en los términos establecidos en la LAP y normativa autonómica reguladora de esta materia con las finalidades previstas en dicha normativa; salvo en lo relativo a los usos de la misma para fines de investigación sanitaria en la modalidad de ensayos clínicos que, como se ha señalado, se rigen por los términos previstos en el Real Decreto de ensayos clínicos con medicamentos. Conforme a las previsiones de esta norma, su intervención como responsable del tratamiento se circunscribe a la autorización para el acceso a la historia clínica del sujeto del ensayo por parte del personal contratado por terceros, como es el caso del monitor o la CRO. Acceso que puede articularse por medio un documento distinto de un contrato y de la figura del encargado del tratamiento, en el que se establezcan las garantías específicas para el desempeño de sus funciones.

Por tanto, los centros hospitalarios sólo actúan como responsables del tratamiento de los datos de la historia clínica que puedan utilizarse en la investigación.

Por todo lo expuesto, en el presente caso, esta Agencia entiende que GETECCU es quien determina los fines y medios de tratamiento de los datos personales de los participantes en el Proyecto ******PROYECTO.1***, al ser el promotor del proyecto en cuestión, por lo que es responsable del tratamiento de los datos personales incluidos en dicha base de datos, que se vio afectada por la brecha de datos personales que dio origen al presente procedimiento.

Por tanto, esta Agencia concluye que GETECCU realiza el tratamiento de los datos personales en el marco del Proyecto ******PROYECTO.1*** 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 19 de junio de 2023, GETECCU notificó a esta Agencia una brecha de datos personales en la que informaba que se había producido un *"Acceso no consentido a archivos del sistema de almacenamiento secundario con borrado y posible descarga de los mismos."*

Por todo lo expuesto, esta Agencia entiende que se habría producido una pérdida de confidencialidad de los datos personales vinculados al Proyecto ******PROYECTO.1***.

Datos personales afectados

El 19 de junio de 2023, GETECCU notificó a esta Agencia una brecha de datos personales en la que informaba que se había visto afectados los siguientes datos personales de (...): ***(…).*** Por su parte, en la ampliación de notificación de brecha de fecha 11 de julio de 2023, GETECCU indicó que se habían visto afectadas por la citada brecha ***(…)*** personas***.***

El 11 de julio de 2023 se recibió en esta Agencia correo electrónico de respuesta por parte de GETECCU en el que afirmaba: "*Se trata de Ficheros CSV con datos estructurados. Los datos personales afectados son: **(…)***.

En su escrito de 21 de febrero de 2024 GETECCU aporta como documento 05.1 copia del contrato de encargo formalizado entre GETECCU y ***CENTRO.54, de 18 de septiembre de 2023, en cuyo anexo I consta:

"Datos objeto de tratamiento:

- *Datos identificativos del paciente: - Nombre - Apellidos - Sexo - Fecha de nacimiento - Número de teléfono - Domicilio.*
- *Datos identificativos del facultativo designado: - Nombre – Apellidos*
- *Datos de salud: - Síntomas - Diagnóstico - Estado físico – Medicación".*

En su escrito de 21 de febrero de 2024, GETECCU adjunta como documento 08 relación con la tipología de datos afectada por la filtración, en el que afirman:

"*Los tipos de datos afectados por el ataque fueron*:

(…)

El 10 de septiembre de 2024 esta Agencia comprueba que en la página web de la Sociedad Valenciana de Farmacia Hospitalaria se obtiene el siguiente documento utilizado en charla formativa sobre el proyecto ******PROYECTO.1***:

*"¿Quién, cuándo y cómo se puede solicitar un proyecto de investigación de ***PROYECTO.1?*
*1. Todos los facultativos de los centros par0cipantes en ***PROYECTO.1 (con autorización del IP del centro)*

2. Socio de GETECCU
3. Para estudios clínicos se deben haber introducido variables clínicas de más de 100 (...), y más de 100 muestras de ADN para estudios genéticos
4. Tener aprobado el estudio que se solicite por parte del CEIC del Hospital al que se pertenezca
5. Cumplimentar un formulario ***(…)****"*

Contiene múltiples capturas de pantalla con los datos que se recaban e introducen en la plataforma por cada investigador, en concreto llama la atención el formulario para introducir los datos demográficos del paciente (página 9 del documento), que incluye los siguientes datos ("*Los campos con asterisco (*) son obligatorios*"): "*Nombre", "Primer Apellido", "Segundo apellido", "Dirección", "Código postal", "Ciudad", Teléfono fijo", "Teléfono móvil", "Número de historia", "Fecha de nacimiento (dd/mm/aaaa) (*)", "Hospital (*)", "Código del paciente (5 dígitos) (*)", "ID del paciente (*)", "Sexo (*)".*

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: ***(…)***. Estos últimos, datos incluidos en el artículo 9 "*Tratamiento de categorías especiales de datos personales*" del RGPD, según el cual: "*1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física*."

Cronología de los hechos y medidas técnicas u organizativas

Junto a la ampliación de notificación de brecha de fecha 11 de julio de 2023, GETECCU
aportó un informe pericial, de fecha 5 de julio de 2023, realizado por la ***ORGANISMO.1, en el que se explicaba que el 14 de junio de 2023 ******EMPRESA.1*** detectó ***(…).***

El informe explica que ******EMPRESA.1 (…).***

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 ***(…),*** entre otras. Y se detallan otras medidas que estaban en marcha o próximas a iniciarse, entre las que destacan: ***(…).***

En su escrito de 21 de febrero de 2024, GETECCU adjunta como documento 06 el análisis de riesgos para la actividad de tratamiento afectada, entre ellas la actividad "*Desarrollo de Proyectos de Investigación Científica en Colaboración con Centros Hospitalarios y de Salud*". En su apartado relativo a "Seguridad del tratamiento", el elemento "Hay acceso no autorizado a datos personales" se le asigna un grado de probabilidad "Improbable", un impacto "Muy significativo" y un riesgo "Muy alto".

Y concluye el documento: "*Tras la evaluación del riesgo realizada teniendo en cuenta la probabilidad de materialización de las amenazas detectadas y el impacto que dicha materialización tendría, se ha podido estimar que el nivel riesgo medio del tratamiento, teniendo en cuenta los datos personales tratados, el contexto y el entorno es MEDIO, para lo que se han aplicado medidas legales, técnicas y de carácter organizativo, de forma que el nivel riesgo, aun no siendo alto, haya sido mitigado.*

En su escrito de 21 de febrero de 2024, GETECCU adjunta como Documento 7 el procedimiento implantado en GETECCU para la gestión de brechas de seguridad, si bien no contiene ni firma ni fecha de creación ni actualización. Su contenido incluye información sobre los canales para comunicar las incidencias y las obligaciones de notificación tanto a AEPD como afectados. Pero no incorpora información sobre tareas, roles y personas responsables de realizarlas.

En su escrito de 21 de febrero de 2024, GETECCU adjunta como documento 10 afirmaciones proporcionadas por ******EMPRESA.1*** aclarando varios puntos del informe pericial. En este documento se explica: ***"(…)".***

Y se afirma que se decidió sustituir los tokens programáticos por roles e implementar un segundo sistema de encriptación en el sistema de almacenamiento secundario (esta nueva funcionalidad se habría implementado desde julio de 2023).

En su escrito de 21 de febrero de 2024, GETECCU adjunta 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", en el que se indica que ***(…)***.

El 18 de abril de 2024 se recibió un segundo escrito por parte de GETECCU, en respuesta a requerimiento de esta Agencia, en el que se adjuntaba como Documento nº 8 la plantilla de contrato entre GETECCU y los centros hospitalarios, *"EXHIBIT C: USE OF TECHNOLOGY AND DATA PROCESSING",* en el que se estipula:

- ***(…)***
- El contrato incluye una tabla descriptiva con los controles y medidas de seguridad a implantar por el prestador encargado de tratamiento (el subrayado es nuestro):

(…)

Por su parte, el 11 de septiembre de 2024 esta Agencia comprueba 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 comprueba 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 comprueba 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* ***(…)*** puede verse el siguiente contenido, entre otro (el subrayado es nuestro):

> *"Un antipatrón común es incrustar claves de acceso de (...) dentro del código fuente, los archivos de configuración o las aplicaciones móviles. Cuando se requiera una clave de acceso de (...) 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 (...) para instancias de (...) , roles de ejecución para funciones* ***(...)****, roles de (...) de* ***(...)*** *para el acceso de usuarios móviles y políticas de* ***(...)*** *para dispositivos IoT.*
> *Cuando interactúe con terceros, es preferible que delegue el acceso a un rol de (...) con el acceso necesario a los recursos de su cuenta en lugar de configurar un usuario de (...) y enviar a ese tercero la clave de acceso secreta para ese usuario."*

El 24 de septiembre de 2024 esta Agencia comprueba 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 ***(…)*** 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.1 (…)****. 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 permitió que la brecha de datos personales se produjera y el mayor impacto de la misma. Las referidas medidas fueron introducidas por el encargado del 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*".

Por todo lo expuesto, esta Agencia entiende que se vio vulnerada la confidencialidad de los datos personales del Proyecto ******PROYECTO.1***, debido a que GETECCU, 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 GETECCU, 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 por la infracción del artículo 5.1.f) del RGPD

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 previamente 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 las posibles infracciones, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa.

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 GETECCU (***(…)*** 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 ***(…)*** personas, debido a no contar con las medidas técnicas u organizativas apropiadas para 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 (...) 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): GETECCU 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 10.000,00 euros.

VII
Obligación incumplida. Encargado del tratamiento

Las previsiones respecto al encargado del tratamiento están recogidas en el artículo 28 del RGPD que estipula lo siguiente:

"1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;
c) tomará todas las medidas necesarias de conformidad con el artículo 32;
d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias

existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del

tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."

Tal y como se ha detallado en el Fundamento de Derecho III del presente documento, al que nos remitimos en aras de brevedad, en las notificaciones de la presente brecha a esta Agencia, GETECCU se identificó como responsable del tratamiento, pero también lo hicieron los centros hospitalarios que notificaron el incidente. Y en estas últimas notificaciones, había discrepancias sobre si había algún encargado de tratamiento implicado en la brecha, y si éste era GETECCU o ******EMPRESA.1***.

En cuanto a los documentos firmados por los centros hospitalarios, en casi todos se les consideraba responsables de tratamiento. Algunos contratos se firmaron directamente con ******EMPRESA.2 /***EMPRESA.1*** como encargado de tratamiento. Otros se firmaron con GETECCU como encargado de tratamiento y se identificó a ******EMPRESA.1*** como subencargado. En otros se identificó a los centros hospitalarios como "*Responsable inicial del Fichero*), a GETECCU como "*Responsable del Fichero-Encargado de Tratamiento"*) y a ******EMPRESA.2*** como subencargado de tratamiento. Y en otros casos no había contrato firmado, sino un documento por el cual el centro se adhería a participar del Proyecto.

De acuerdo con las Directrices 07/2020 del EDPB sobre los conceptos de «Responsable del Tratamiento» y «Encargado del Tratamiento» en el RGPD, esta Agencia analizó la realidad de los hechos para dilucidar el verdadero rol de cada una de las entidades participantes en el citado Proyecto y concluyó que GETECCU en realidad era la responsable de tratamiento de la base de datos del Proyecto ******PROYECTO.1***, mientras que los centros hospitalarios y ******EMPRESA.1*** actúan como encargados de tratamiento.

No obstante, en los documentos que rigen las relaciones entre los centros hospitalarios y GETECCU ello no se ve reflejado ni, en consecuencia, se incluyen los extremos a que obliga el artículo 28.3 del RGPD.

La atribución errónea de los roles de responsable y encargado del tratamiento supone la falta de una atribución clara de responsabilidades entre ambas figuras, impidiendo al responsable del tratamiento cumplir con las obligaciones que le impone el RGPD para procurar la protección debida respecto de los datos personales que se tratan por su cuenta en relación con el control de proceso de entrega que lleva a cabo.

Por otra, desde el punto de vista de los interesados, cuyos datos están siendo tratados, dicha omisión también tiene consecuencias: el contrato entre el responsable del tratamiento y su encargado es un elemento que no solo articula jurídicamente la relación entre dos partes (responsable y encargado del tratamiento) sino que cumple una función de garantía de los derechos y libertades de los interesados.

En este sentido, el contrato de tratamiento debe prever, entre otros aspectos, que:

- Los datos únicamente sean tratados siguiendo las instrucciones documentadas del responsable del tratamiento. Lo que supone una doble garantía para los interesados: existencia de unas instrucciones documentadas por parte del

responsable y obligación del encargado de tratar los datos personales siguiendo dichas instrucciones.

- Los empleados del encargado que traten los datos personales de los interesados han de respetar la confidencialidad.

- El encargado ha de adoptar todas las medidas necesarias de conformidad con el artículo 32 del RGPD.

- El encargado del tratamiento no puede recurrir a otro encargado sin la autorización previa por escrito, específica o general del responsable.

- El encargado tiene la obligación de suprimir o devolver los datos personales al responsable una vez que finalice la prestación de los servicios del tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.

En conclusión, dicho contrato regula y ordena cómo se va a desarrollar la relación entre el responsable y su encargado del tratamiento con el claro objetivo de brindar una adecuada protección de los derechos y libertades de los interesados, cuyos datos se están tratando. Lo cual no ha tenido lugar en las relaciones que rigen entre GETECCU y los centros hospitalarios que forman parte del Proyecto ******PROYECTO.1***.

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 GETECCU, por vulneración del artículo 28 del RGPD.

VIII
Tipificación de la infracción del artículo 28 del RGPD y calificación a efectos de prescripción

El artículo 83.4 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

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 73 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes: (…)

> *k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679."*

IX
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 previamente 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 las posibles infracciones, 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 GETECCU (***(...)*** 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 no contar los documentos que rigen la relación entre GETECCU y los centros hospitalarios la información exigida por el artículo 28 del RGPD, lo cual afecta al menos a ***(…)*** personas hasta la actualidad.
- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): los datos objeto del tratamiento son datos de salud de los (...) 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): GETECCU 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 28 del RGPD, permite fijar inicialmente una sanción de multa administrativa de 7.000,00 euros.

X
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 28 del RGPD, Artículo 5.1.f) del RGPD y Artículo 32 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 GETECCU 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 adopción de las medidas técnicas u organizativas apropiadas para garantizar una seguridad adecuada de los datos personales, necesarias para garantizar el cumplimiento de lo dispuesto en el artículo 5.1.f) del RGPD.

- Acreditar la realización de los correspondientes contratos de encargado de tratamiento con los centros hospitalarios participantes en el Proyecto ***PROYECTO.1, que cumplan con los extremos exigidos por el artículo 28 del RGPD.

La imposición de esta medida 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 **GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)**, con NIF **G07762669**, por la presunta infracción del artículo 5.1.f) y artículo 28 del RGPD, tipificadas, respectivamente, en el artículo 83.5 y 83.4 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 17.000,00 euros, sin perjuicio de lo que resulte de la instrucción:

- Por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, multa administrativa de 10.000,00 euros.
- Por la presunta infracción del artículo 28 del RGPD, tipificada en el artículo 83.4 del RGPD, multa administrativa de 7.000,00 euros.

QUINTO: NOTIFICAR el presente acuerdo a **GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU),** con NIF **G07762669**, 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 **13.600,00** 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 **13.600,00** 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 **10.200,00 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 **(13.600,00** euros o **10.200,00 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.

1479-111124

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

>>

SEGUNDO**:** En fecha 16 de enero de 2025, ***GETECCU*** ha procedido al pago de la sanción en la cuantía de **10.200,00 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**:** ***GETECCU*** 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 reglamentariamente."

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 **10.200,00 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, ***GETECCU*** 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 **17.000,00 euros.**
Tras haber procedido ***GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)*** 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 **10.200,00 euros**.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202310012**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)*** 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 ***GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)***.

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 ***GRUPO ESPAÑOL DE TRABAJO EN ENFERMEDAD DE CHRON Y COLITIS ULCEROSA (GETECCU)***,

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