- **Expediente N.º: PS/00268/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ASOCIACION DE CONSUMIDORES Y USUARIOS EN ACCION DE MADRID FACUA, (en adelante, FACUA), con fecha 14 de junio de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E*, (*en adelante CONSEJERIA). Los motivos en que basa la reclamación son los siguientes:

-Que, a causa de un error de programación, han quedado al descubierto datos de carácter personal (DNI, número de teléfono, fecha de nacimiento y números de identificación sanitaria) de los ciudadanos al acceder a la web de autocita, activada por la Comunidad de Madrid el 24 de mayo. Esta plataforma de la Comunidad de Madrid ha sido creada para que los ciudadanos que aún no habían recibido ninguna dosis de la vacuna contra la COVID-19 pudieran programar una cita para su vacunación, según ha podido comprobar el medio de comunicación digital EL DIARIO.ES.

Junto a la reclamación se aporta pantallazo de la página de inicio de la aplicación autocita COVID de la Consejería de Sanidad de la Comunidad Autónoma de Madrid, y la noticia publicada por elDiaro.es el día 15/06/2021, que incluye un pantallazo de los datos que aparecen en dicha aplicación, si bien en el adjuntado como ejemplo se han anonimizado todos excepto el nombre “A.A.A.”.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de la reclamación presentada por FACUA a la CONSEJERIA, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 18/06/2021 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 10 de septiembre de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la FACUA .

CUARTO: 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 VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

ENTIDAD INVESTIGADA

Durante las presentes actuaciones se ha investigado la siguiente entidad:

CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E con domicilio en C/ MELCHOR FERNÁNDEZ ALMAGRO, Nº 1 - 28029 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha de 10 de junio de 2021, el medio digital ElDiario.es publica un artículo en el que se informaba, entre otros, de lo siguiente:

> *"La Comunidad de Madrid activó el pasado 24 de mayo su sistema de autocita por franjas de edad para que los ciudadanos que aún no habían recibido ninguna dosis de la vacuna contra la COVID-19 pudieran programar una cita. Desde ese día y hasta este jueves, la página web habilitada por la Consejería de Sanidad para pedir esa citación ha tenido una brecha de seguridad que ha afectado a todas las personas con una tarjeta sanitaria de la región, según ha podido comprobar elDiario.es.*
>
> *A causa de un error de programación, la página dejaba a la vista el nombre completo, DNI, número de teléfono, fecha de nacimiento y los números de identificación sanitaria tanto autonómicos como nacionales de cualquier ciudadano cuando se hacía una solicitud de cita con su número CIPA (Código de Identificación Personal de la Comunidad de Madrid)."*

Dicho artículo publica además lo que aduce que son los datos de un ciudadano afectado por la brecha de seguridad del portal de "autocita" para vacunarse contra el coronavirus de la Comunidad de Madrid, en el que se aprecia que en el código web aparecen tachados los datos correspondientes a los siguientes campos: NIF, nombre, apellido1, apellido2, fecha de nacimiento, número de teléfono, sexo y los números de identificación sanitaria tanto autonómicos como nacionales.

En la imagen publicada por el medio de comunicación se aprecia que en la pestaña "red", dentro de la herramienta de inspección del navegador, un JSON (notación de objeto de JavaScript, es un formato de texto sencillo para el intercambio de datos) en el que aparecen los datos anteriormente mencionados con el contenido ocultado intencionadamente.

El artículo además menciona que esa información no era visible a simple vista, sino que estaba presente en el código informático de la Web y que para acceder a ella había que activar las herramientas para desarrolladores del navegador, una opción que está disponible para cualquier usuario pero que no se suele utilizar sin ciertos conocimientos técnicos previos.

También informa de que la brecha ha sido cerrada después de recibir un aviso por parte del medio de comunicación.

2.- Con fecha de 5 de octubre de 2021 se solicitó por la inspección de datos a la CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, en adelante la Consejería, la siguiente documentación e información:

1. *Descripción detallada y cronológica de los hechos ocurridos.*
2. *Especificación detallada de las causas que han hecho posible el incidente.*
3. *Número de personas afectadas por la violación de la seguridad de los datos personales.*
4. *Categoría de los datos personales involucrados.*
5. *Posibles consecuencias para las personas afectadas.*
6. *Descripción detallada de las acciones tomadas para solucionar el incidente y minimizar su impacto sobre las personas afectadas.*

7. *Medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente, así como la documentación acreditativa del Análisis de Riesgos que ha conllevado la implantación de dichas medidas de seguridad y, en su caso, copia de las Evaluaciones de Impacto de los tratamientos donde se ha producido la violación de seguridad de los datos personales.*
8. *Copia del Registro de Actividad de los tratamientos donde se ha producido el incidente.*
9. *Si la violación de seguridad ha sido notificada a las personas afectadas, indique el canal utilizado, fecha de la comunicación y detalle del mensaje enviado. En caso negativo, indicar los motivos.*
10. *Motivo por el cual no se ha notificado la brecha antes de las 72 horas de que sucediera.*
11. *Cualquier otra que considere relevante.*

Dicho requerimiento fue notificado mediante el servicio de Dirección Electrónica Habilitada Única y fue aceptada por el destinatario el día 10 de octubre de 2021, según acredita dicho servicio.

El día 21 de octubre de 2021 se recibe escrito del Comité Delegado de Protección de Datos de la Consejería solicitando una ampliación de plazo para responder a la solicitud.

3.- Trascurrido el plazo dado para responder a la solicitud de información sin obtener respuesta, con fecha 1 de diciembre de 2021 se reiteró la solicitud de información a la Consejería, a través del servicio de Dirección Electrónica Habilitada Única y fue aceptada por el destinatario el día 2 de diciembre de 2021, según acredita dicho servicio.

4.- Ante la falta de respuesta a los requerimientos de la inspección de datos, con fecha 14 de marzo de 2022 la Directora de la Agencia Española de Protección de Datos acuerda el inicio de un procedimiento sancionador a la Consejería, por la infracción del artículo 58.1 del Reglamento General de Protección de Datos (RGPD), tipificada en el art. 83. 5 e) del citado RGPD, en el marco del cual, el organismo reclamado alega que el Comité Delegado de Protección de Datos de la Consejería, en el ejercicio de sus funciones, remitió respuesta al requerimiento de la inspección de datos mediante escrito de fecha 01 de febrero de 2022 con referencia de Registro de presentación REGAGE22e00002434053 y aporta documentación justificante de presentación en el registro y copia del escrito de atención al requerimiento de información, en el que ponen de manifiesto lo siguiente:

Respecto de las causas que han hecho posible el incidente:

- Tras analizar los hechos concluyen que el fallo detectado relacionado con este sistema de información se debe a una exposición de información de datos personales (públicos) accedidos mediante una cookie de sesión válida, y editando la URL accedida uno de los campos de entrada llamado “idPaciente” con un DNI válido. De esta forma, se pueden visualizar una serie de datos personales correspondientes a la persona con el DNI utilizado. Adicionalmente se detecta que la aplicación web contaba con mecanismos de bloqueo insuficientes ante reintentos a la hora de introducir los datos de autenticación (Código de Identificación Poblacional Autonómico [CIPA], Fecha de nacimiento y DNI) para solicitar la cita.

Respecto de los datos afectados

- No se tiene constancia en la Consejería de Sanidad de que el fallo ocurrido haya afectado a ningún ciudadano, más allá de la información publicada en los medios de comunicación. Así mismo, no se tiene constancia de que se haya producido daño alguno en las libertades y derechos de los ciudadanos.
- Únicamente podrían haberse visto afectados datos de carácter identificativo de los ciudadanos: Nombre y Apellidos, CIPA, Fecha de nacimiento, ID del paciente, DNI, Número de teléfono, Sexo.
- No se tiene constancia en la Consejería de Sanidad que se haya producido un daño en las libertades y derechos de los ciudadanos, sin que se haya constatado hasta la fecha que se haya derivado en un perjuicio material o inmaterial en los ciudadanos que pudieran haberse visto afectados. La subsanación de esta vulnerabilidad fue previa a su difusión en medios de comunicación.

Descripción detallada de las acciones tomadas para solucionar el incidente y minimizar su impacto sobre las personas afectadas:

- Se procedió a realizar la modificación del aplicativo con la finalidad de mejorar el sistema de información y se procedió a la subida de versión, siendo los siguientes cambios los más relativos:

  Día 9 de junio:

  □ Reducir al mínimo la información a intercambiar entre el navegador del usuario y el servidor. Solo se transmite información que se muestra por pantalla o que el usuario ha introducido previamente. No se intercambia en ningún caso número de teléfono, CIP SNS (Código de Identificación Poblacional del Sistema Nacional de Salud), sexo. El resto (fecha nacimiento, nombre y apellidos), se muestran por pantalla.

  □ Solicitar el código de verificación enviado por SMS como primer paso, nada más introducir los datos de identificación.

  □ No devolver código de errores específicos, sólo genéricos.

  □Se aumentan los datos requeridos en el proceso de identificación, ofreciendo dos posibilidades al usuario:

  o CIPA + Fecha nacimiento + DNI

  o DNI/NIE/PASAPORTE + Fecha nacimiento + Primer apellido

- El diseño de la arquitectura de la aplicación no permite la modificación de los datos de filiación del usuario. Debido a que el aplicativo hace uso de una base de datos independiente y el móvil solicitado es únicamente usado como parte del OTP implementado para validar la petición de cita.

Respecto a las medidas de seguridad

- El equipo de desarrollo del SERMAS utiliza una metodología de desarrollo actualizada continuamente recogido en ***(…)*** en la Consejería de Sanidad de la Comunidad de Madrid.

  Aportan copia de ***(…)***, cuyo objetivo es disponer de los estándares que deben cumplir las aplicaciones desde el punto de vista técnico y funcional, así como los documentos técnicos que describen las plataformas con los que deben integrarse

las mismas. Las indicaciones y directrices ***(…)*** son de obligado cumplimiento para todos los desarrollos de nuevas aplicaciones para la DGSIS.

- El punto ***(…)*** establece respecto del acceso a las aplicaciones de los ciudadanos lo siguiente:

  (…)

- Manifiestan en relación con la evaluación de impacto (EIPD) sobre el presente tratamiento, teniendo en cuenta su naturaleza, alcance, contexto y fines, así como que en el presente tratamiento no se produce una evaluación sistemática y exhaustiva de aspectos personales que se base en un tratamiento automatizado, ni existe un tratamiento de las categorías especiales de datos. Por lo tanto, se considera que en el presente tratamiento no resulta necesario la realización de una EIPD.

5.- Se ha verificado por la inspección de datos que en Internet Archive (biblioteca digital gestionada por una organización sin ánimo de lucro que contienen millones de páginas de Internet grabadas desde 1996) tiene registrada la página web https://autocitavacuna.sanidadmadrid.org existente en la fecha de 14 de junio de 2021, en la que se puede comprobar que para solicitar cita para la vacuna se solicita solamente el código CIPA y en caso de no disponer de dicho código se solicita DNI y fecha de nacimiento.

CONCLUSIONES

- Respecto de las causas que han hecho posible el incidente publicado en ElDiario.es, el representante de la Consejería manifiesta que, tras analizar los hechos concluyen que el fallo detectado relacionado con este sistema de información se debe a una exposición de información de datos personales (públicos) accedidos mediante una cookie de sesión válida, y editando la URL accedida uno de los campos de entrada llamado "idPaciente" con un DNI válido. Esta explicación no concuerda con el incidente de seguridad comunicado a esta Agencia por FACUA, incidente por el que los datos personales quedaban expuestos cuando se hacía una solicitud de cita con un número CIPA (Código de Identificación Personal de la Comunidad de Madrid) existente. Se ha comprobado por la inspección de datos que Internet Archive conserva la página web https://autocitavacuna.sanidadmadrid.org existente en la fecha de 14 de junio de 2021, en la que se puede comprobar que para solicitar cita para la vacuna se solicita solamente el código CIPA y en caso de no disponer de dicho código se solicita DNI y fecha de nacimiento.

  Por otra parte, el representante de la Consejería reconoce que, entre las acciones tomadas para solucionar el incidente, se ha reducido al mínimo la información a intercambiar entre el navegador del usuario y el servidor. Solo se transmite información que se muestra por pantalla o que el usuario ha introducido previamente. No se intercambia en ningún caso número de teléfono, CIP SNS (Código de Identificación Poblacional del Sistema Nacional de Salud), sexo. El resto (fecha nacimiento, nombre y apellidos), se muestran por pantalla. Además, se han aumentan los datos requeridos en el proceso de identificación, ofreciendo dos posibilidades al usuario: CIPA + Fecha nacimiento + DNI o DNI/NIE/PASAPORTE + Fecha nacimiento + Primer apellido.

- Respecto a las medidas de seguridad, el Servicio Madrileño de Salud (SERMAS) dependiente de la Consejería, utiliza una metodología de desarrollo de aplicaciones informáticas que se recoge en ***(…)*** de la Comunidad de Madrid.

  - El ***(…)*** relativo a la autenticación establece respecto del acceso a las aplicaciones de los ciudadanos lo siguiente:

    (…)

    Se ha comprobado por la inspección de datos que Internet Archive conserva la página web https://autocitavacuna.sanidadmadrid.org existente en la fecha de 14 de junio de 2021, en la que se puede comprobar que para solicitar cita para la vacuna se solicita solamente el código CIPA y en caso de no disponer de dicho código se solicita DNI y fecha de nacimiento.

  - El ***(…)*** denominado ***(…)*** establece, entre otros, lo siguiente:

    (…)

    Se desconoce si la Consejería ha llevado a cabo un análisis de riesgos, según establece la metodología ***(…).***

  - El mismo ***(…)*** establece lo siguiente:

    (…)

> Se desconoce si se han llevado a cabo las pruebas y análisis pertinentes de este tratamiento por la Oficina de Seguridad, según establece la metodología ***(…).***

QUINTO: Con fecha 15 de julio de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 5.1.f) del RGPD, Artículo 33 del RGPD, Artículo 25 del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

Notificado el Acuerdo de Inicio, la CONSEJERIA presentó escrito de alegaciones en el que en síntesis manifestaba:

-Que en los meses de mayo y junio de 2021, nos encontrábamos en un momento muy crítico relacionado con la gestión de la pandemia. En este periodo, en el que se abre el proceso de vacunación a la población en general -si bien de manera escalonada por franjas de edad-, se requería de manera urgente la organización y la apertura de dicho proceso de manera masiva y, en consecuencia, resultaba necesario ofrecer un sistema con información clara y sencilla sobre el proceso a seguir por parte de la ciudadanía y la premura que requería su adopción a nivel organizativo, incluyendo también varios canales para facilitar las citaciones de la ciudadanía.
Este estado de emergencia sanitaria provocó que resultase necesario desarrollar un gran número de nuevas herramientas con gran celeridad para poder prestar el mejor servicio a los ciudadanos mediante el desarrollo y despliegue del proceso de citación para vacunación de manera ágil en los centros habilitados, incluso permitiendo al ciudadano seleccionar la hora y centro de su preferencia, lo que facilitó que la Comunidad de Madrid alcanzase un elevado número de población vacunada, contribuyendo con dicha acción a que se pudiese hacer frente a esta coyuntura de pandemia lo antes posible, y facilitar la movilidad de la población antes del inicio de periodos considerados tradicionalmente como vacacionales en los que se producirían la movilidad de la población.

> -A este respecto, esta Agencia recuerda que, tanto el artículo 25.1 del RGPD como el 32 del mismo texto legal, inciden en la necesidad de que, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, el responsable adopte medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos y garantizar un nivel de seguridad adecuado al riesgo, sin que pueda aceptarse como eximente la circunstancia de premura alegada por emergencia sanitaria. No cabe apreciar, en el presente caso, estado de necesidad que justifique la puesta en producción de una aplicación defectuosa, que permitía el acceso a datos personales de un elevado número de ciudadanos, sin realizar previamente las comprobaciones necesarias para determinar su correcto funcionamiento, y cuyo uso puede ocasionar un mal mayor que aquel que se pretende evitar.

-Que en el acuerdo de inicio se hace referencia en el apartado “Respecto a las medidas de seguridad” al punto ***(…),*** que es genérico, y que para Autocita se habilitaron otros procedimientos de acceso para que los ciudadanos que no dispusieran de Tarjeta Sanitaria de la Comunidad de Madrid, pudieran solicitar la

vacunación a través de la página web. Consideran, por tanto, que la referencia ***(…)*** debería suprimirse puesto que no mantiene relación con este caso concreto.

> -A este respecto, esta Agencia simplemente ha reflejado la información facilitada por la propia CONSEJERIA en su respuesta al requerimiento de información efectuado por la AEPD, en el que adjuntan un ***(…)*** a la que hacen referencia en el apartado 6 de su respuesta:
>
> *"6. Medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente, así como la documentación acreditativa del Análisis de Riesgos que ha conllevado la implantación de dichas medidas de seguridad y, en su caso, copia de las Evaluaciones de Impacto de los tratamientos donde se ha producido la violación de seguridad de los datos personales".*
>
> Y que, según indica la propia CONSEJERIA, es la metodología de desarrollo utilizada.

-Que se han establecido medidas para la mejora continua de la gestión de las crisis y ciberincidencias, centradas en la prevención, detección y respuesta a incidentes de seguridad. En concreto, se han implementado las siguientes medidas destinadas a reforzar la seguridad:

• Se ha revisado el proceso de desarrollo y puesta en producción de aplicativos, como parte del proceso de mejora continua en el ciclo de desarrollo y puesta en marcha de aplicativos, poniendo especial énfasis en los siguientes aspectos:

> o Refuerzo de los recursos destinados a la validación previa de la seguridad del aplicativo antes de la entrada en producción.
> o Refuerzo de los métodos de realización de pruebas de penetración y análisis código a todos los sistemas de desarrollo propio y no se pondrán en producción hasta con solventar las posibles vulnerabilidades detectadas.
> o Reevaluación de todos los sistemas de desarrollo propio para comprobar que se hayan subsanado las vulnerabilidades con tipología Alta o Crítica, detectadas durante la fase de "pentest".

• Se ha revisado la ***(…),*** actualizado las principales áreas a tener en cuenta a la hora de desarrollar aplicaciones, así como las tareas primordiales tareas a tener en cuenta a la hora de implementar aplicaciones en la estructura de Integración Continua y Despliegue Continuo en la CSCM, con el objeto de disponer de los estándares más actualizados que deben cumplir las aplicaciones desde el punto de vista técnico y funcional, así como los documentos técnicos que describen las plataformas con los que deben integrarse las mismas.

• Se han mejorado los casos de uso en auditorías de seguridad.

Por último, resulta relevante mencionar que en la actualidad se está trabajando en un proyecto de adopción de una herramienta ***(…)***.

> -A este respecto, esta Agencia valora positivamente la adopción de nuevas medidas que redunden en una mayor seguridad en lo que al tratamiento de datos personales se refiere y que puedan prevenir, en un futuro, incidentes como el que se sustancia en el presente procedimiento.

-Que la ***(…)*** forma parte del cuerpo normativo de seguridad de la CSCM y se encuentra calificada como documento de USO RESTRINGIDO, por lo que se considera un documento de difusión controlada y su uso se restringe a personal interno de la organización, puesto que su difusión pública puede suponer un riesgo para la seguridad. El contenido ***(…)*** constituye información confidencial cuya difusión, fuera de la organización o del ámbito de las personas que no requieran conocer dicha información, puede provocar que se perjudique o se produzcan ciberataques en los servicios considerados esenciales por la legislación.
Por tanto se requiere que tal información, dada su extraordinaria sensibilidad, sea objeto de reserva y, en consecuencia, que no se muestre información del contenido ***(…)*** en la Resolución que recaiga en el presente procedimiento y que pudiera, en su caso, ser objeto de publicación.

> -A este respecto, esta Agencia manifiesta que la documentación obrante en el expediente se utiliza exclusivamente para realizar una exhaustiva y correcta instrucción del mismo, no siendo, en ningún caso, de acceso público. Incluso en el supuesto de que en la resolución que recaiga obre algún tipo de información de uso restringido, se procedería a su anonimización como paso previo a su publicación.

SEXTO: Con fecha 12 de agosto de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a CONSEJERÍA DE SANIDAD, con NIF S7800001E,

-Por la una infracción del Artículo 5.1.f) del RGPD, tipificado en el artículo 83.5 del RGPD, con un apercibimiento.

-Por una infracción del Artículo 25 del RGPD, tipificado en el artículo 83.4 el RGPD, con un apercibimiento.

-Por una infracción del Artículo 32 del RGPD, tipificado en el artículo 83.4 el RGPD, con un apercibimiento.

-Por una infracción del Artículo 33 del RGPD, tipificado en el artículo 83.4 el RGPD, con un apercibimiento.

SEPTIMO: Notificada la propuesta de resolución, la CONSEJERIA presenta un nuevo escrito de alegaciones en el que, en síntesis, reproduce las ya presentadas al Acuerdo de Inicio, y añade que:

– De la notificación a la AEPD. Como se señaló en el primer escrito remitido a la AEPD en relación al presente procedimiento sancionador, en función del nivel de riesgo de la incidencia, teniendo en cuenta el bajo volumen de datos que podrían haberse afectado, la tipología de los mismos, siendo únicamente datos de carácter

identificativo, y el impacto inexistente provocado en los interesados, se estimó que no resultaba preceptivo informar a la Autoridad de Control.
Así pues, el artículo 33 del RGPD señala que “En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas”.

Por ello, en el presente supuesto, como hemos señalado, teniendo en cuenta que, ni en ese momento, ni actualmente, se tiene constancia de que ningún ciudadano haya sufrido consecuencias negativas en sus derechos y libertades, teniendo en consideración adicionalmente que no se han visto afectados un número significativos de datos personales, ni se han visto afectados datos de categoría especial de los ciudadanos, se estimó en su momento que dicha comunicación no era necesaria puesto que era improbable que se constituyese un riesgo para los derechos y libertados de los ciudadanos.

– Medidas de seguridad tomadas inicialmente. Además de lo anterior, como se indicó en la comunicación inicial a la AEPD, desde el diseño la herramienta contaba con medidas de seguridad adecuadas para evitar, tanto que el impacto de posibles incidentes de seguridad fuera elevado, como que sucediesen los mismos.

Así pues, en el primer escrito remitido ya se indicaba que en todo momento el canal de comunicación entre el usuario y los servidores del SERMAS están securizados. El diseño de la arquitectura de la aplicación no permite la modificación de los datos de filiación del usuario. Debido a que el aplicativo hace uso de una base de datos independiente y el móvil solicitado es únicamente usado como parte del OTP (One Time Password) implementado para validar la petición de cita.

De igual forma y para subsanar lo ocurrido, una vez se tuvo conocimiento del fallo e identificado el mismo, antes de que se viera publicado en los medios de comunicación, se procedió a realizar la modificación del aplicativo con la finalidad de mejorar el sistema de información y se procedió a la subida de versión, siendo los siguientes cambios los más relativos:

Día 9 de junio:
(…)

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Consta acreditado que con fecha 24/05/2021, la CONSEJERIA activó un sistema de autocita para que los ciudadanos pudieran solicitar cita para vacunarse contra la COVID-19.

SEGUNDO: Consta acreditado que hubo un fallo en el sistema, debido al cual quedaban expuestos datos personales (públicos) accediendo mediante una cookie de

sesión válida, y editando la URL accedida uno de los campos de entrada llamado "idPaciente" con un DNI válido.

TERCERO: Consta acreditado que la aplicación web contaba con mecanismos de bloqueo insuficientes ante reintentos a la hora de introducir los datos de autenticación.

CUARTO: Consta acreditado que, tras tener conocimiento de la brecha de seguridad, la CONSEJERIA no lo comunico a la AEPD.

FUNDAMENTOS DE DERECHO

I

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 y 48.1 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.

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

En relación a las alegaciones presentadas a la propuesta de resolución, la CONSEJERIA reitera las ya presentadas anteriormente y añade que:

1-Con respecto a la notificación de la brecha a la AEPD, en función del nivel de riesgo de la incidencia, teniendo en cuenta el bajo volumen de datos que podrían haberse afectado, la tipología de los mismos, siendo únicamente datos de carácter identificativo, y el impacto inexistente provocado en los interesados, se estimó que no resultaba preceptivo informar a la Autoridad de Control.

En el presente supuesto, teniendo en cuenta que, ni en ese momento, ni actualmente, se tiene constancia de que ningún ciudadano haya sufrido consecuencias negativas en sus derechos y libertades, teniendo en consideración adicionalmente que no se han visto afectados un número significativos de datos personales, ni se han visto afectados datos de categoría especial de los ciudadanos, se estimó en su momento que dicha comunicación no era necesaria puesto que era improbable que se constituyese un riesgo para los derechos y libertados de los ciudadanos.

> -A este respecto esta Agencia indica que no se ha presentado por parte de la CONSEJERIA una valoración de riesgos realmente efectuada, resultando, por tanto, muy indeterminado el concepto de: "*era improbable que se constituyese un riesgo para los derechos y libertados de los ciudadanos*"

2- Medidas de seguridad tomadas inicialmente. Además de lo anterior, como se indicó en la comunicación inicial a la AEPD, desde el diseño la herramienta contaba con

medidas de seguridad adecuadas para evitar, tanto que el impacto de posibles incidentes de seguridad fuera elevado, como que sucediesen los mismos.

> -A este respecto, esta Agencia constata que, de hecho, los incidentes si llegaron a materializarse, que se detectó un fallo en el sistema, debido a una exposición de información de datos personales (públicos) accedidos mediante una cookie de sesión válida, y editando la URL accedida uno de los campos de entrada llamado "idPaciente" con un DNI válido.
> Adicionalmente se constató que la aplicación web contaba con mecanismos de bloqueo insuficientes ante reintentos a la hora de introducir los datos de autenticación.

III

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"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»)."

En el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos de la CONSEJERIA, fueron indebidamente expuestos a un tercero, según consta en la noticia publicada en elDiario.es.

De la instrucción llevada a cabo en el presente procedimiento se concluye que la CONSEJERIA ha vulnerado lo establecido en el artículo 5.1.f del RGPD.

IV

La infracción se tipifica en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes 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; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. 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. (…)"

V

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

(…)
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

VI

El artículo 25.1 del RGPD indica:

"*1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados*."

En el presente caso consta que se ha detectado un fallo en el sistema, debido a una exposición de información de datos personales (públicos) accedidos mediante una cookie de sesión válida, y editando la URL accedida uno de los campos de entrada llamado "idPaciente" con un DNI válido. Adicionalmente se detecta que la aplicación web contaba con mecanismos de bloqueo insuficientes ante reintentos a la hora de introducir los datos de autenticación.

De la instrucción llevada a cabo en el presente procedimiento se concluye que la CONSEJERIA ha vulnerado lo establecido en el artículo 25.1 del RGPD,

VII

La infracción se tipifica en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones 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; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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:

> *(…)*
> *d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679. (…)*

VIII

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *(…)*
> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local. (…)*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se

ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

(…)
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

IX

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, en el momento de producirse la brecha, la CONSEJERIA no contaba con las medidas técnicas y organizativas apropiadas para evitar que se produjera un incidente como el que se sustancia en el presente procedimiento, ya que una vez introducido el código CIPA no se requería una segunda autentificación, ni los datos personales aparecían seudonimizados.

De la instrucción llevada a cabo en el presente procedimiento se concluye que la CONSEJERIA ha vulnerado lo establecido en el artículo 32 del RGPD,

X

La infracción se tipifica en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones 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; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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:

> *(…)*
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*
> *(…)*

XI

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

(…)

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

XII

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número

aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, consta que la CONSEJERIA ha sufrido una brecha de seguridad de los datos personales en fecha 24/05/2021 y no ha informado a esta Agencia.

De la instrucción llevada a cabo en el presente procedimiento se concluye que la CONSEJERIA ha vulnerado lo establecido en el artículo 33 del RGPD.

XIII

La infracción se tipifica en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones 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; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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:

(…)
r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679. (…)"

XIV

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

(…)

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

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

PRIMERO: IMPONER a CONSEJERÍA DE SANIDAD, con NIF S7800001E,

-Por la una infracción del Artículo 5.1.f) del RGPD, tipificado en el artículo 83.5 del RGPD, una sanción de apercibimiento.

-Por una infracción del Artículo 25 del RGPD, tipificado en el artículo 83.4 el RGPD, una sanción de apercibimiento.

-Por una infracción del Artículo 32 del RGPD, tipificado en el artículo 83.4 el RGPD, una sanción de apercibimiento.

-Por una infracción del Artículo 33 del RGPD, tipificado en el artículo 83.4 el RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a CONSEJERÍA DE SANIDAD.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 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.

938-120722

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